ESET MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

Installation Manual and User Guide

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Click here to download the most recent version of this document

ENJOY SAFER TECHNOLOGY™

ESET **MAIL SECURITY**

Copyright ©2016 by ESET, spol. s r.o.
ESET Mail Security was developed by ESET, spol. s r.o.

For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care: www.eset.com/support

REV. 19/05/2016

Contents

1. Introduction 6

1.1 What's new in version 6? 6
1.2 Help pages 7
1.3 Methods used 7
1.3.1 Mailbox database protection 8
1.3.2 Mail transport protection 8
1.3.3 On-demand database scan 8
1.4 Types of protection 10
1.4.1 Antivirus protection 10
1.4.2 Antispam protection 10
1.4.3 Application of user-defined rules 11
1.5 User interface 11
1.6 Managed via ESET Remote Administrator 12
1.6.1 ERA Server 12
1.6.2 Web Console 13
1.6.3 Agent 13
1.6.4 RD Sensor 14
1.6.5 Proxy 14

2. System requirements 15

3. Installation 16

3.1 ESET Mail Security installation steps 17
3.1.1 Command line installation 20
3.1.2 Installation in cluster environment 22
3.2 Product activation 23
3.3 Terminal Server 23
3.4 ESET AV Remover 24
3.5 Upgrading to a newer version 24
3.6 Exchange Server Roles - Edge vs Hub 24
3.7 Exchange Server 2013 Roles 25
3.8 POP3 Connector and antispam 25

4. Beginner's guide 26

4.1 The user interface 26
4.2 Log files 28
4.2.1 Scan log 30
4.3 Scan 31
4.3.1 Hyper-V scan 32
4.4 Mail Quarantine 34
4.4.1 Quarantined mail details 36
4.5 Update 37
4.5.1 Setting up virus DB update 38
4.5.2 Configuring Proxy server for updates 38
4.6 Setup 39
4.6.1 Server 39
4.6.2 Computer 40
4.6.3 Tools 42
4.6.4 Import and export settings 43
4.7 Tools 44
4.7.1 Running processes 45
4.7.2 Watch activity 46
4.7.2.1 Time period selection 47
4.7.3 ESET Log Collector 47
4.7.4 Protection statistics 48
4.7.5 Cluster 50
4.7.5.1 Cluster wizard - page 1 51
4.7.5.2 Cluster wizard - page 2 53
4.7.5.3 Cluster wizard - page 3 54
4.7.5.4 Cluster wizard - page 4 56
4.7.6 ESET Shell 59
4.7.6.1 Usage 61
4.7.6.2 Commands 64
4.7.6.3 Batch files / Scripting 66
4.7.7 ESET SysInspector 67
4.7.7.1 Create a computer status snapshot 67
4.7.7.2 ESET SysInspector 67
4.7.7.2.1 Introduction to ESET SysInspector 67
4.7.7.2.1.1 Starting ESET SysInspector 68
4.7.7.2.2 User Interface and application usage 68
4.7.7.2.2.1 Program Controls 68
4.7.7.2.2.2 Navigating in ESET SysInspector 70
4.7.7.2.2.1 Keyboard shortcuts 71
4.7.7.2.2.3 Compare 72
4.7.7.2.3 Command line parameters 73
4.7.7.2.4 Service Script 74
4.7.7.2.4.1 Generating Service script 74
4.7.7.2.4.2 Structure of the Service script 74
4.7.7.2.4.3 Executing Service scripts 77
4.7.7.2.5 FAQ 77
4.7.7.2.6 ESET SysInspector as part of ESET Mail Security 79
4.7.8 ESET SysRescue Live 79
4.7.9 Scheduler 79
4.7.10 Submit samples for analysis 82
4.7.10.1 Suspicious file 83
4.7.10.2 Suspicious site 83
4.7.10.3 False positive file 83
4.7.10.4 False positive site 83
4.7.10.5 Other 84
4.7.11 Quarantine 84
4.8 Help and support 85
4.8.1 How to 86
4.8.1.1 How to update ESET Mail Security 86
4.8.1.2 How to activate ESET Mail Security 86
4.8.1.3 How does ESET Mail Security count mailboxes 87
4.8.1.4 How to create a new task in Scheduler 87
4.8.1.5 How to schedule a scan task (every 24 hours) 88
4.8.1.6 How to remove a virus from your server 88
4.8.2 Submit support request 88
4.8.3 ESET Specialized Cleaner 88
4.8.4 About ESET Mail Security 89

4.8.5 Product activation 89
4.8.5.1 Registration 90
4.8.5.2 Security Admin activation 90
4.8.5.3 Activation failure 90
4.8.5.4 License 90
4.8.5.5 Activation progress 90
4.8.5.6 Activation successful 91

5. Working with ESET Mail Security 92

5.1 Server 93
5.1.1 Agent priority setup 94
5.1.1.1 Modify priority 94
5.1.2 Agent priority setup 94
5.1.3 Antivirus and antispyware 95
5.1.4 Antispam protection 96
5.1.4.1 Filtering and verification 97
5.1.4.2 Advanced settings 98
5.1.4.3 Greylisting settings 101
5.1.5 Rules 103
5.1.5.1 Rules list 103
5.1.5.1.1 Rule wizard 104
5.1.5.1.1.1 Rule condition 105
5.1.5.1.1.2 Rule action 106
5.1.6 Mail transport protection 107
5.1.6.1 Advanced settings 109
5.1.7 Mailbox database protection 110
5.1.8 On-demand database scan 111
5.1.8.1 Additional mailbox items 112
5.1.8.2 Proxy server 113
5.1.8.3 Database scan account details 113
5.1.9 Mail Quarantine 114
5.1.9.1 Local quarantine 115
5.1.9.1.1 File storage 116
5.1.9.1.2 Web interface 117
5.1.9.2 Quarantine mailbox and MS Exchange quarantine 121
5.1.9.2.1 Quarantine manager settings 121
5.1.9.2.2 Proxy server 122
5.1.9.3 Quarantine manager account details 123

5.2 Computer 123
5.2.1 An infiltration is detected 124
5.2.2 Processes exclusions 125
5.2.3 Automatic exclusions 125
5.2.4 Shared local cache 126
5.2.5 Performance 126
5.2.6 Real-time file system protection 126
5.2.6.1 Exclusions 127
5.2.6.1.1 Add or Edit exclusion 128
5.2.6.1.2 Exclusion format 128
5.2.6.2 ThreatSense parameters 128
5.2.6.2.1 File extenstions excluded from scanning 131
5.2.6.2.2 Additional ThreatSense parameters 131
5.2.6.2.3 Cleaning levels 131
5.2.6.2.4 When to modify real-time protection configuration 132
5.2.6.2.5 Checking real-time protection 132
5.2.6.2.6 What to do if real-time protection does not work 132
5.2.6.2.7 Submission 132
5.2.6.2.8 Statistics 133
5.2.6.2.9 Suspicious files 133
5.2.7 On-demand computer scan and Hyper-V scan 134
5.2.7.1 Custom scan and Hyper-V scan launcher 134
5.2.7.2 Scan progress 136
5.2.7.3 Profile manager 137
5.2.7.4 Scan targets 138
5.2.7.5 Pause a scheduled scan 138
5.2.8 Idle-state scanning 138
5.2.9 Startup scan 139
5.2.9.1 Automatic startup file check 139
5.2.10 Removable media 139
5.2.11 Document protection 140
5.2.12 HIPS 140
5.2.12.1 HIPS rules 141
5.2.12.1.1 HIPS rule settings 142
5.2.12.2 Advanced setup 143
5.2.12.2.1 Drivers always allowed to load 143

5.3 Update 144
5.3.1 Update rollback 145
5.3.2 Update mode 145
5.3.3 HTTP Proxy 145
5.3.4 Connect to LAN as 146
5.3.5 Mirror 147
5.3.5.1 Updating from the Mirror 148
5.3.5.2 Mirror files 149
5.3.5.3 Troubleshooting Mirror update problems 150
5.3.6 How to create update tasks 150

5.4 Web and email 150
5.4.1 Protocol filtering 151
5.4.1.1 Excluded applications 151
5.4.1.2 Excluded IP addresses 151
5.4.1.3 Web and email clients 151
5.4.2 SSL/TLS 152
5.4.2.1 Encrypted SSL communication 152
5.4.2.2 List of known certificates 153
5.4.3 Email client protection 153
5.4.3.1 Email protocols 154
5.4.3.2 Alerts and notifications 154
5.4.3.3 MS Outlook toolbar 155
5.4.3.4 Outlook Express and Windows Mail toolbar 155
5.4.3.5 Confirmation dialog 155
5.4.3.6 Rescan messages 155
5.4.4 Web access protection 156
5.4.4.1 Basic 156
5.4.4.2 URL address management 157
5.4.4.2.1 Create new list 157
5.4.4.2.2 Address list 158

Contents

5.4.5 Anti-Phishing protection 158

5.5 Device control 160

5.5.1 Device control - Rules editor 160
5.5.2 Adding Device control rules 161
5.5.3 Detected devices 162
5.5.4 Device groups 162

5.6 Tools 162

5.6.1 ESET LiveGrid 163
5.6.1.1 Exclusion filter 164
5.6.2 Quarantine 164
5.6.3 Microsoft Windows update 164
5.6.4 WMI Provider 164
5.6.4.1 Provided data 165
5.6.4.2 Accessing Provided Data 169
5.6.5 ERA scan targets 169
5.6.6 Log files 169
5.6.6.1 Log filtering 171
5.6.6.2 Find in log 171
5.6.7 Proxy server 172
5.6.8 Email notifications 172
5.6.8.1 Message format 173
5.6.9 Presentation mode 173
5.6.10 Diagnostics 174
5.6.11 Customer Care 174
5.6.12 Cluster 175

5.7 User interface 176

5.7.1 Alerts and notifications 177
5.7.2 Access setup 178
5.7.2.1 Password 178
5.7.2.2 Password setup 178
5.7.3 Help 178
5.7.4 ESET Shell 178
5.7.5 Disable GUI on Terminal Server 179
5.7.6 Disabled messages and statuses 179
5.7.6.1 Confirmation messages 179
5.7.6.2 Disabled application statuses 179
5.7.7 System tray icon 179
5.7.7.1 Pause protection 180
5.7.8 Context menu 180

5.8 Revert all settings in this section 181

5.9 Revert to default settings 181

5.10 Scheduler 182

5.10.1 Task details 183
5.10.2 Task timing - Once 183
5.10.3 Task timing 183
5.10.4 Task timing - Daily 184
5.10.5 Task timing - Weekly 184
5.10.6 Task timing - Event triggered 184
5.10.7 Task details - Run application 184
5.10.8 Task details - Send mail quratine reports 184
5.10.9 Skipped task 184
5.10.10 Scheduler task details 185
5.10.11 Scheduler task - Background scan 185
5.10.12 Update profiles 185
5.10.13 Creating new tasks 185

5.11 Quarantine 186

5.11.1 Quarantining files 187
5.11.2 Restoring from Quarantine 187
5.11.3 Submitting file from Quarantine 187

5.12 Operating system updates 188

6. Glossary 189

6.1 Types of infiltration 189

6.1.1 Viruses 189
6.1.2 Worms 189
6.1.3 Trojan horses 190
6.1.4 Rootkits 190
6.1.5 Adware 190
6.1.6 Spyware 191
6.1.7 Packers 191
6.1.8 Exploit Blocker 191
6.1.9 Advanced Memory Scanner 191
6.1.10 Potentially unsafe applications 192
6.1.11 Potentially unwanted applications 192

6.2 Email 192

6.2.1 Advertisements 193
6.2.2 Hoaxes 193
6.2.3 Phishing 193
6.2.4 Recognizing spam scams 193
6.2.4.1 Rules 194
6.2.4.2 Bayesian filter 194
6.2.4.3 Whitelist 194
6.2.4.4 Blacklist 195
6.2.4.5 Server-side control 195

1. Introduction

ESET Mail Security 6 for Microsoft Exchange Server is an integrated solution that protects mailboxes from various types of malicious content including email attachments infected by worms or trojans, documents containing harmful scripts, phishing schemes and spam. ESET Mail Security provides three types of protection: Antivirus, Antispam and user-defined rules. ESET Mail Security filters the malicious content at the mail server level, before it arrives in the recipient's email client inbox.

ESET Mail Security supports Microsoft Exchange Server versions 2003 and later, as well as Microsoft Exchange Server in a cluster environment. In newer versions (Microsoft Exchange Server 2003 and later), specific roles (mailbox, hub, edge) are also supported. You can remotely manage ESET Mail Security in larger networks with the help of ESET Remote Administrator.

While providing Microsoft Exchange Server protection, ESET Mail Security also includes tools to ensure the protection of the server itself (resident protection, web-access protection and email client protection).

1.1 What's new in version 6?

- Mail quarantine manager - Administrator can inspect objects in this storage section and decide to delete or release them. This feature offers simple management of emails quarantined by the transport agent.
- Mail Quarantine Web interface - A web-based alternative to Mail quarantine manager.
- Antispam - This essential component went through a major redesign and is now using brand new award winning engine with improved performance.
- On-demand database scan - On-demand database scanner uses the EWS (Exchange Web Services) API to connect to Microsoft Exchange Server via HTTP/HTTPS. Also, the scanner runs parallel scanning to improve the performance.
- Rules - The Rules menu item allows administrators to manually define email filtering conditions and actions to take with filtered emails. Rules in the latest version of ESET Mail Security were redesigned to allow for greater flexibility giving the user even more possibilities.
- ESET Cluster - Similar to ESET File Security 6 for Microsoft Windows Server, joining workstations to nodes will offer additional automation of management due to the ability to distribute one configuration policy across all cluster members. The creation of clusters themselves is possible using the node installed, which can then install and initiates all nodes remotely. ESET server products are able to communicate with each other and exchange data such as configuration and notifications, and can synchronize data necessary for proper operation of a group of product instances. This allows for the same configuration of the product for all members of a cluster. Windows Failover Clusters and Network Load Balancing (NLB) Clusters are supported by ESET Mail Security. Additionally, you can add ESET Cluster members manually without the need for a specific Windows Cluster. ESET Clusters work in both domain and workgroup environments.
- Storage scan - scans all shared files on a local server. This makes it easy to selectively scan only user data that is stored on the file server.
- Component-based installation - you can choose which components you want to add or remove.
- Processes exclusions - excludes specific processes from Antivirus on-access scanning. Due to the critical role of dedicated servers (application server, storage server, etc.) regular backups are mandatory to guarantee timely recovery from fatal incidents of any kind. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level antivirus protection are used during backup. Similar problems can occur when attempting live migrations of virtual machines. The only effective way to avoid both situations is to deactivate antivirus software. By excluding specific process (for example those of the backup solution) all file operations attributed to such excluded process are ignored and considered safe, thus minimizing interference with the backup process. We recommend that you use caution when creating exclusions – a backup tool that has been excluded can access infected files without triggering an alert which is why extended permissions are only allowed in the real-time protection module.

- ESET Log Collector - automatically gathers information such as ESET Mail Security configuration and numerous logs. ESET Log Collector will make it easy for you to collect diagnostic information needed to help ESET technicians quickly resolve an issue.
- eShell (ESET Shell) - eShell 2.0 is now available in ESET Mail Security. eShell is a command line interface that offers advanced users and administrators more comprehensive options to manage ESET server products.
- Hyper-V scan - Is a new technology that allows for scanning of Virtual Machine (VM) disks on Microsoft Hyper-V Server without the need of any "Agent" on the particular VM.
- Better integration with ESET Remote Administrator including the ability to schedule On-demand scan.

1.2 Help pages

Dear valued customer, we are glad to welcome you to ESET Mail Security. This guide is intended to help you make the best use of ESET Mail Security.

Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by browsing the **Contents** of the help pages. Alternatively, you can use the **Index** to browse by keywords or use full-text **Search**.

To learn more about any window in the program, press **F1** on your keyboard while you have the given window open. The help page related to the window you are currently viewing will be displayed.

ESET Mail Security allows you to search help topics by keyword or by typing words or phrases to search for within the User Guide. The difference between these two methods is that a keyword may be logically related to help pages which do not contain that particular keyword in the text. Searching by words and phrases will search the content of all pages and display only those containing the searched word or phrase in the actual text.

1.3 Methods used

The following three methods are used to scan emails:

- Mailbox database protection - formerly known as Mailbox scanning via VSAPI. This type of protection is only available for Microsoft Exchange Server 2010, 2007 and 2003 operating in the Mailbox Server (Microsoft Exchange 2010 and 2007) or Back-End server (Microsoft Exchange 2003) role. This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it includes the Mailbox or Back-End role).
- Mail transport protection - formerly known as Message filtering on the SMTP server level. This protection is provided by the transport agent and is only available for Microsoft Exchange Server 2007 or newer operating in the Edge Transport Server or Hub Transport Server role. This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles).
- On-demand database scan - allows you to execute or schedule an Exchange mailbox database scan. This feature is only available for Microsoft Exchange Server 2007 or newer operating in the Mailbox server or Hub Transport role. This also applies to a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles). See Exchange Server 2013 roles for some specifics regarding roles in Exchange 2013.

1.3.1 Mailbox database protection

The mailbox scanning process is triggered and controlled by the Microsoft Exchange Server. Emails in the Microsoft Exchange Server store database are scanned continuously. Depending on the version of Microsoft Exchange Server, the VSAPI interface version and the user-defined settings, the scanning process can be triggered in any of the following situations:

- When the user accesses email, for example, in an email client (email is always scanned with the latest virus signature database)
- In the background, when use of the Microsoft Exchange Server is low
- Proactively (based on the Microsoft Exchange Server's inner algorithm)

The VSAPI interface is currently used for antivirus scan and rule-based protection.

1.3.2 Mail transport protection

SMTP server-level filtering is secured by a specialized plugin. In Microsoft Exchange Server 2000 and 2003, the plugin in question (Event Sink) is registered on the SMTP server as a part of Internet Information Services (IIS). In Microsoft Exchange Server 2007/2010, the plugin is registered as a transport agent on the Edge or the Hub roles of the Microsoft Exchange Server.

SMTP server-level filtering by a transport agent provides protection in the form of antivirus, antispam and user-defined rules. As opposed to VSAPI filtering, SMTP server-level filtering is performed before the scanned email arrives in the Microsoft Exchange Server mailbox.

1.3.3 On-demand database scan

Since running a full email database scan in large environments could result in undesired system load, you can choose which databases and which mailboxes therein will be scanned. You can filter scan targets further by specifying the time-stamp of messages to scan to minimize impact on server system resources.

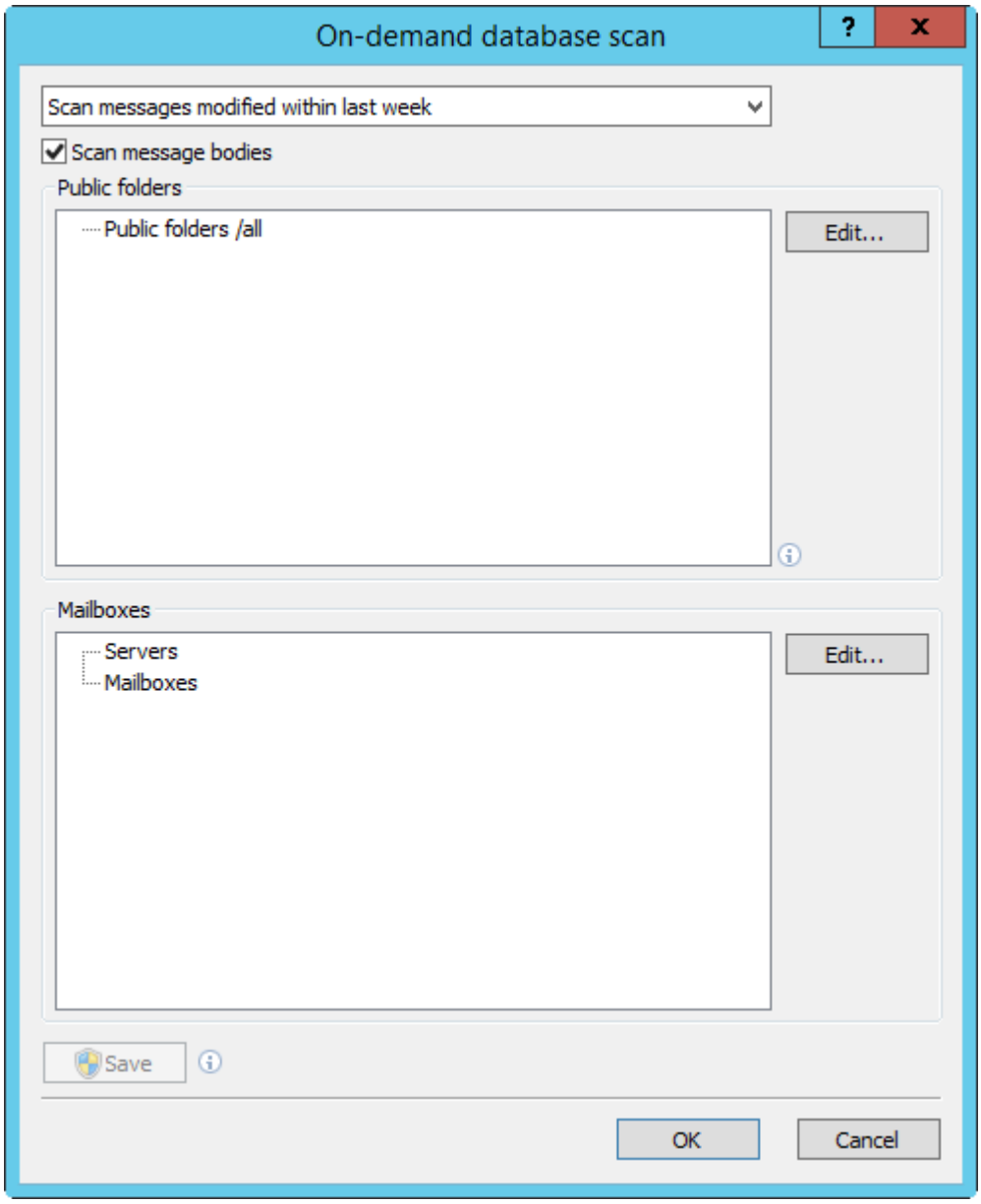
The following item types are scanned in both Public folders and in user Mailboxes:

- Email
- Post
- Calendar items (meetings/appointments)
- Tasks
- Contacts
- Journal

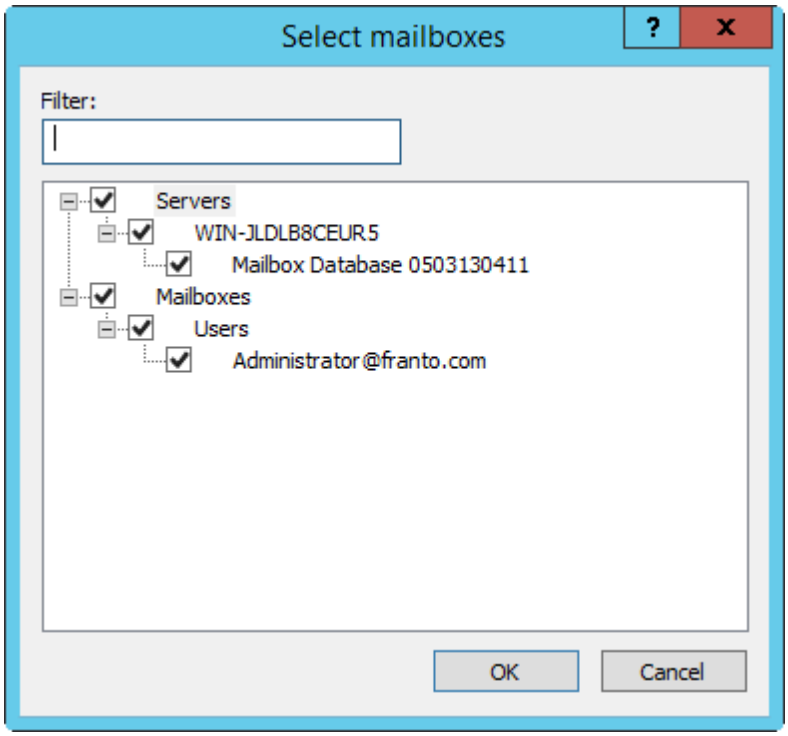
You can use the drop-down list to choose which messages to scan according to their time-stamp. For example, messages modified within the last week. You can also choose to scan all messages if required.

Select the check box next to **Scan message bodies** to enable or disable message body scanning.

Click **Edit** to select the public folder that will be scanned.


On-demand database scan
Scan messages modified within last week
Scan message bodies
Public folders
Public folders /all
Edit...
Mailboxes
Servers
Mailboxes
Edit...
Save
OK
Cancel

Select the check box(es) next to Server Databases and Mailboxes you want to scan. **Filter** lets you find Databases and Mailboxes quickly, especially if there are a large number of mailboxes in your Exchange infrastructure.



Click **Save** to save your scan targets and parameters to the On-demand scan profile.

1.4 Types of protection

There are three types of protection:

- Antivirus protection
- Antispam protection
- Application of user-defined rules

1.4.1 Antivirus protection

Antivirus protection is one of the basic functions of ESET Mail Security . Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by blocking it and then cleaning it, deleting it, or moving it to Quarantine.

1.4.2 Antispam protection

Antispam protection incorporates multiple technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting, etc.) to maximize detection of email threats. The antispam scanning engine produces a probability value in the form of a percentage (0 to 100) for each scanned email message.

ESET Mail Security can also use the Greylisting method (disabled by default) of spam filtering. This method relies on the RFC 821 specification, which states that since SMTP is considered an unreliable transport protocol, every message transfer agent (MTA) should repeatedly attempt to deliver an email after encountering a temporary delivery failure. Many spam messages are delivered once to a bulk list of email addresses generated automatically. Greylisting calculates a control value (hash) for the envelope sender address, the envelope recipient address and the IP address of the sending MTA. If the server cannot find the control value for the triplet within its own database, it refuses to accept the message and returns a temporary failure code (for example, 451). A legitimate server will attempt redelivery of the message after a variable time period. The triplet's control value will be stored in the database of verified connections on the second attempt, allowing any email with relevant characteristics to be delivered from then on.

1.4.3 Application of user-defined rules

Protection based on rules is available for scanning with both the VSAPI and the transport agent. You can use the ESET Mail Security user interface to create individual rules that may also be combined. If one rule uses multiple conditions, the conditions will be linked using the logical operator AND. Consequently, the rule will be executed only if all its conditions are met. If multiple rules are created, the logical operator OR will be applied, meaning the program will run the first rule for which the conditions are met.

In the scanning sequence, the first technique used is greylisting - if it is enabled. Consequent procedures will always execute the following techniques: protection based on user-defined rules, followed by an antivirus scan and, lastly, an antispam scan.

1.5 User interface

ESET Mail Security has a graphical user interface (GUI) designed to be as intuitive as possible. The GUI gives users quick and easy access to the main functions of the program.

In addition to the main GUI, the **Advanced setup window** is accessible from anywhere in the program by pressing the **F5** key.

From the Advanced setup window, you can configure settings and options based on your needs. The menu on the left consists of the following categories: **Server**, **Computer**, **Update**, **Web and email**, **Device control**, **Tools** and **User interface**. Some of the main categories contain subcategories. When you click an item (category or subcategory) in the menu on the left, the respective settings for that item are shown on the right pane.

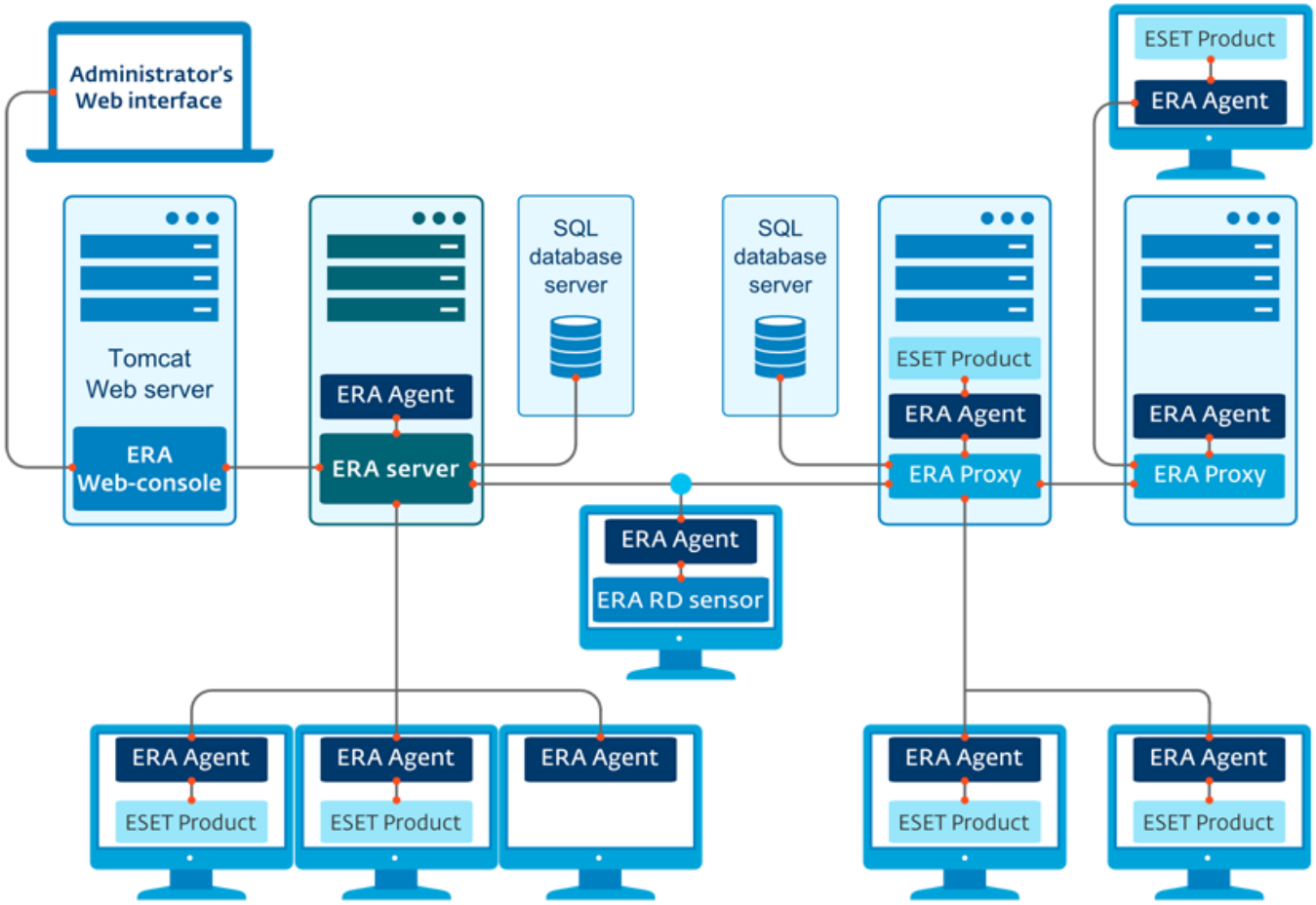
For more detailed information about the GUI click here.

1.6 Managed via ESET Remote Administrator

ESET Remote Administrator (ERA) is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Remote Administrator task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Remote Administrator does not provide protection against malicious code on its own, it relies on the presence of ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, OS X and operating systems that run on mobile devices (mobile phones and tables).

The picture below depicts a sample architecture for a network protected by ESET security solutions manged by ERA:



NOTE: For more information about ERA, see the ESET Remote Administrator Online Help.

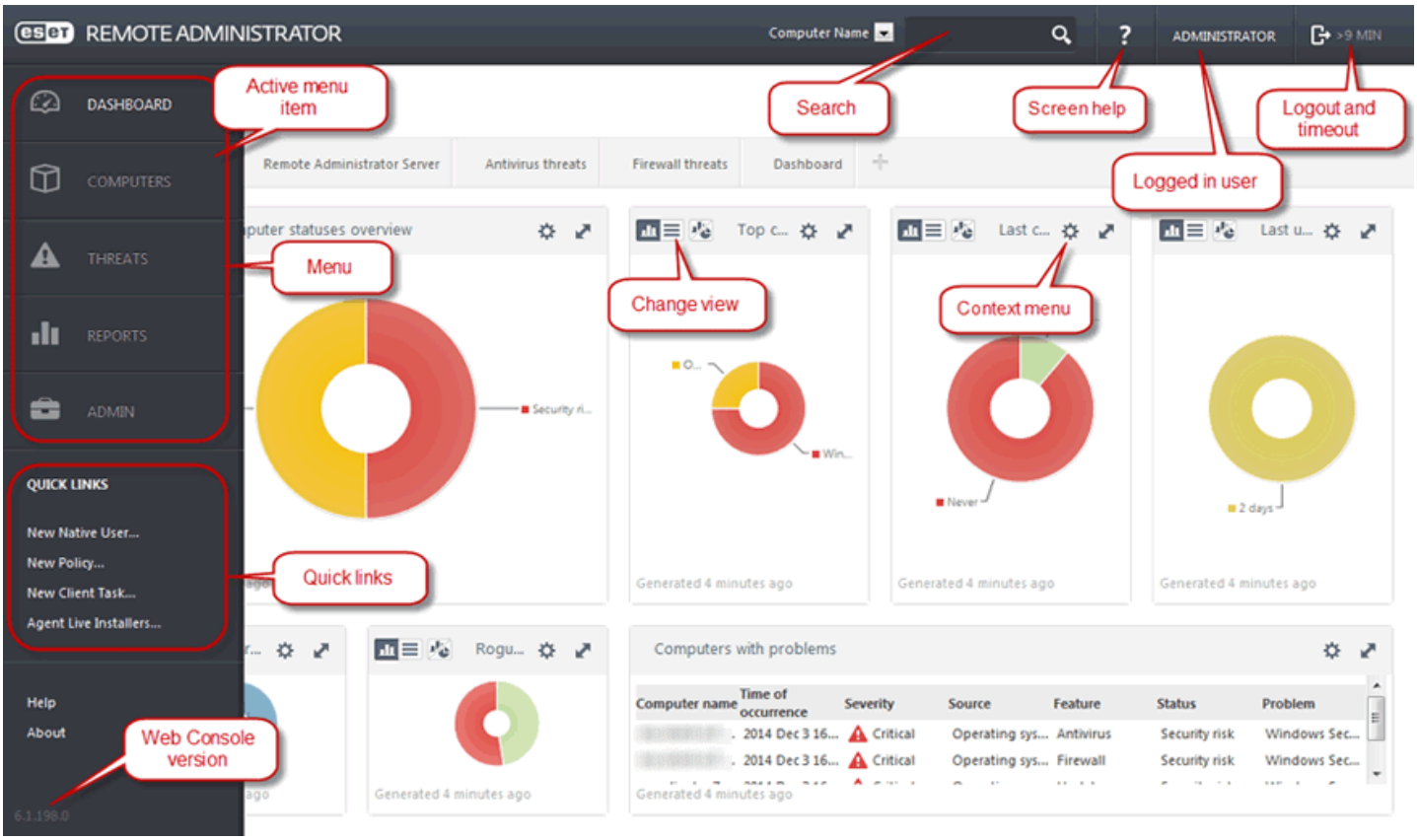
1.6.1 ERA Server

ESET Remote Administrator Server is a primary component of ESET Remote Administrator. It is the executive application that processes all data received from clients that connect to the Server (through the ERA Agent). The ERA Agent facilitates communication between the client and the server. Data (Client logs, configuration, agent replication, etc.) are stored in a database. To correctly process the data, the ERA Server requires a stable connection to a Database server. We recommend that you install ERA Server and your database on separate servers to optimize performance. The machine on which ERA Server is installed, must be configured to accept all Agent/Proxy/RD Sensor connections which are verified using certificates. Once ERA Server is installed, you can open ERA Web Console which connects to the ERA Server (as shown in the diagram). From the Web Console, all ERA Server operations are performed when managing ESET security solution within your network.

1.6.2 Web Console

ERA Web Console a web-based user interface that presents data from ERA Server and allows you to manage ESET security solutions in your environment. The Web Console can be accessed using a browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. If you decide to make the web server accessible from the Internet, then you have the advantage of being able to use ESET Remote Administrator from nearly any place and any device with an active Internet connection.

This is the Web Console Dashboard:



Within the top bar of the Web Console is the **Quick Search** tool. Select **Computer Name**, **IPv4/IPv6 Address** or **Threat Name** from the drop-down menu, type your search string into the text field and click the magnifier symbol or press **Enter** to search. You will be redirected to the **Groups** section, where your search result will be displayed - a client or a list of clients. All clients are managed via the Web Console. You can access the Web Console using most common devices and browsers.

NOTE: For more information see ESET Remote Administrator Online Help.

1.6.3 Agent

ERA Agent is an essential part of the ESET Remote Administrator product. An ESET product on a client machine (for example ESET Endpoint security for Windows) communicates with ERA Server through the Agent. This communication allows for the management of the ESET products on all remote clients from a one central location. The Agent collects information from the client and sends it to the Server. If the Server sends a task for the client, the task is sent to the Agent and the Agent sends this task to the client. All network communication happens between the Agent and the upper part of the ERA network - Server and Proxy.

NOTE: For more information see ESET Remote Administrator Online Help.

The ESET Agent uses one of the following three methods to connect to the Server:

1. The Client's Agent is directly connected to the Server.
2. The Client's Agent is connected through a Proxy that is connected to the Server.
3. The Client's Agent is connected to the Server through multiple Proxies.

The ESET Agent communicates with ESET solutions installed on a client, collects information from programs on that client and passes configuration information received from the Server to the client.

NOTE: The ESET Proxy has its own Agent, which handles all communication tasks between clients, other proxies and the Server.

1.6.4 RD Sensor

RD (Rogue Detection) Sensor is a search tool for computers on the network. RD Sensor is a part of ESET Remote Administrator and is designed to detect machines on your network. It offers a convenient way of adding new computers to ESET Remote Administrator without the need to add them manually. Every computer that is found on your network is displayed in the Web Console. From here, you can take further actions with individual client computers.

RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. The ERA Server then evaluates whether the PCs found on the network are unknown to ERA server or already managed.

NOTE: For more information see ESET Remote Administrator Online Help.

1.6.5 Proxy

ERA Proxy is another component of ESET Remote Administrator, and serves two purposes. In the case of a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies facilitating the main ERA Server. The other advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that the ERA Agent on each client is not connecting to the main ERA Server directly via ERA Proxy which is on the same local network of the branch office. Therefore freeing up the link to the branch office. The ERA Proxy accepts connections from all local ERA Agents, sums their data up and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

Depending on your network configuration, it is possible for ERA Proxy to connect to another ERA Proxy and then connect to the main ERA Server.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

NOTE: For example of deployment scenario for ERA Proxy see ESET Remote Administrator Online Help.

2. System requirements

Supported Operating Systems:

- Microsoft Windows Server 2003 SP2 (x86 and x64)
- Microsoft Windows Server 2003 R2 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

NOTE: Minimum supported OS is Microsoft Windows Server 2003 SP2.

Supported Microsoft Exchange Server versions:

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

Hardware requirements depend on the operating system version in use. We recommend reading the Microsoft Windows Server product documentation for more detailed information on hardware requirements.

3. Installation

After purchasing ESET Mail Security, the installer can be downloaded from ESET's website (www.eset.com) as an .msi package.

Please note that you need to execute the installer under Built-in Administrator account or a domain Administrator account (in case you have local Built-in Administrator account disabled). Any other user, despite being a member of Administrators group, will not have sufficient access rights. Therefore you need to use Built-in Administrator account, as you will not be able to successfully complete the installation under any other user account than local or domain Administrator.

There are two ways to execute the installer:

- You can login locally using Administrator account credentials and simply run the installer
- You can be logged in as other user, but need to open command prompt with Run as... and type in Administrator account credentials to have the cmd running as Administrator, then type in the command to execute the installer (e.g. msiexec /i emsx_nt64_ENU.msi but you need to replace emsx_nt64_ENU.msi with the exact file name of the msi installer you have downloaded)

Once you launch the installer and accept End-User License Agreement (EULA) the installation wizard will guide you through the setup. If you choose not to accept the terms in the License Agreement, the wizard will not continue.

Complete
This is the recommended installation type. It will install all features of ESET Mail Security. After choosing of this type of installation you will only specify folders where to install the product, but you can simply accept predefined default installation folders (recommended). Installer the installs all program features automatically.

Custom
Custom installation type lets you choose program features of ESET Mail Security that will be installed on your system. You will see a typical list of features/components which you select from for the installation.

In addition to wizard installation, you can choose to install ESET Mail Security silently via command line. This installation type does not require any interaction such as when using wizard described above. It is useful for instance for automating or streamlining. This type of installation is also called unattended since it does not prompt user to do an action.

Silent / Unattended installation
Complete installation via command line: `msiexec /i <packagename> /qn /l*xv msi.log`

NOTE: We highly recommend installing ESET Mail Security on a freshly installed and configured OS, if possible. However, if you do need to install it on an existing system, the best to do is to uninstall previous version of ESET Mail Security, restart the server and install the new ESET Mail Security afterwards.

NOTE: If you have previously used other third-party antivirus software on your system, we recommend you to uninstall it completely prior to the installation of ESET Mail Security. To do this, you can use ESET AV Remover which makes the uninstallation easier.

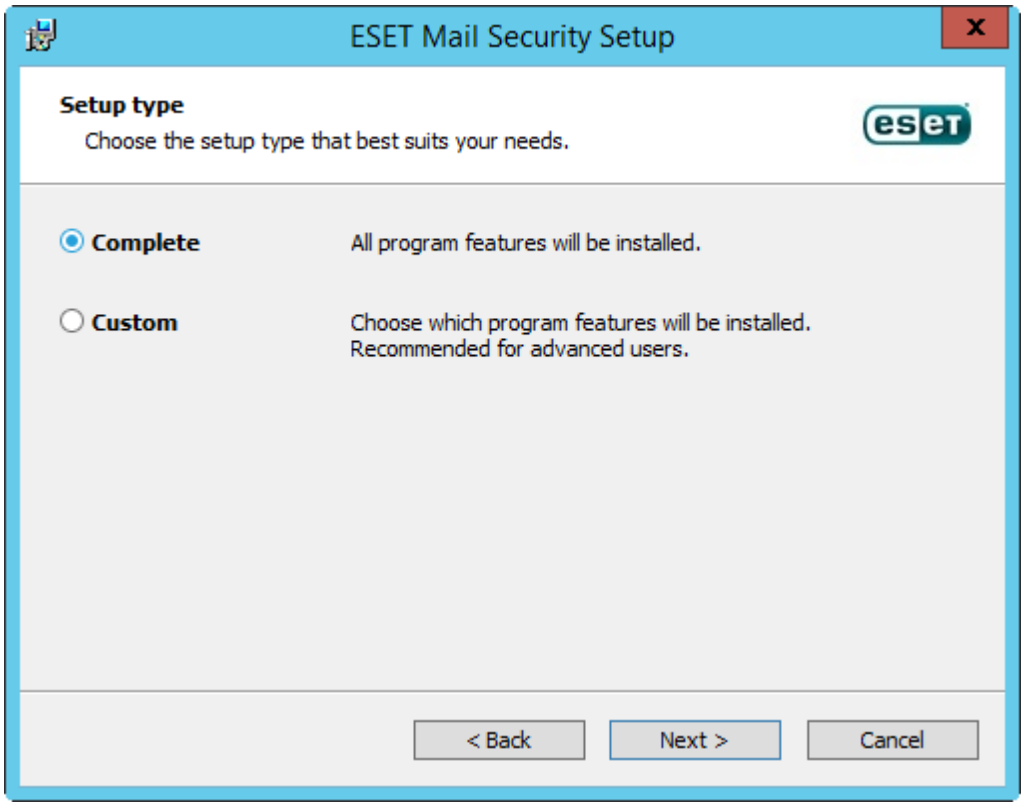
3.1 ESET Mail Security installation steps

Follow the steps below to install ESET Mail Security using the Setup Wizard:

ESET Mail Security Setup
MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
Welcome to ESET Mail Security Setup Wizard
The Setup Wizard will install ESET Mail Security on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
It is important that you uninstall any other security applications such as antivirus, antispyware or firewall before you continue with the installation. They can conflict with this product, possibly resulting in serious problems.
6.2.10009.3
< Back
Next >
Cancel

After accepting the EULA, select one of the following installation types:

- **Complete** - Install all ESET Mail Security features. This is the recommended installation type.
- **Custom** - Select which ESET Mail Security features will be installed on your system.


ESET Mail Security Setup
Setup type
Choose the setup type that best suits your needs.
Complete
All program features will be installed.
Custom
Choose which program features will be installed. Recommended for advanced users.
< Back
Next >
Cancel

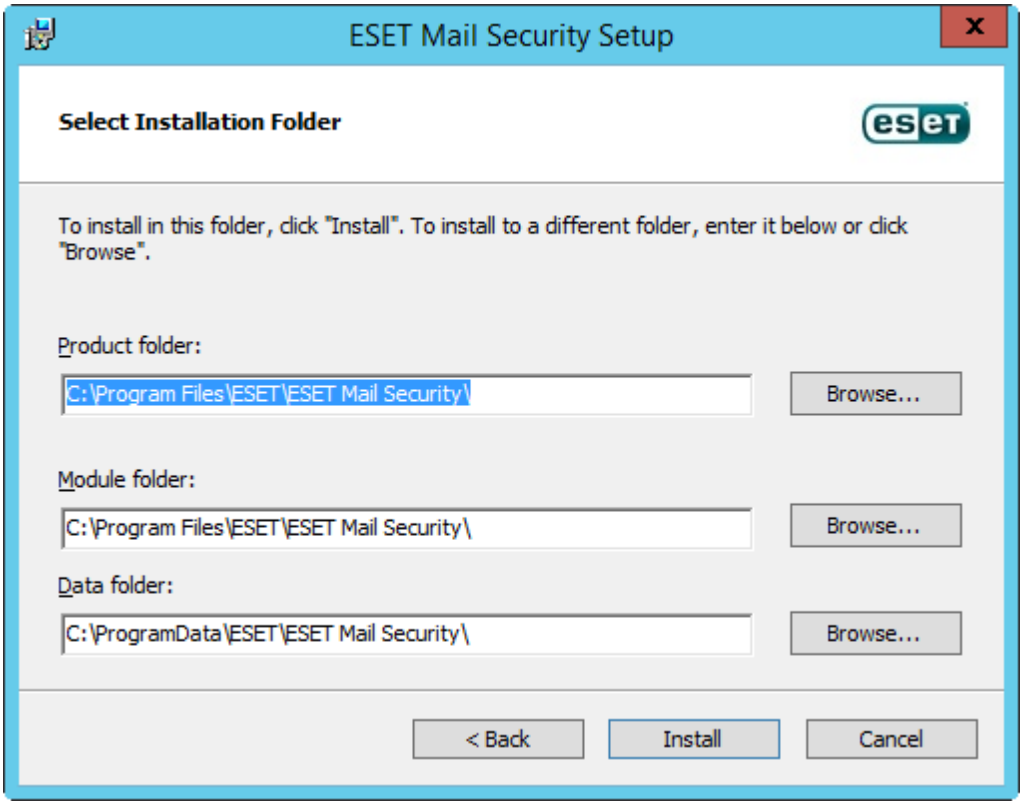
Complete installation:

Also called full installation. This will install all ESET Mail Security components. You will be prompted to select the

location where ESET Mail Security will be installed. By default, the program installs in C:\Program Files\ESET\ESET Mail Security. Click **Browse** to change this location (not recommended).

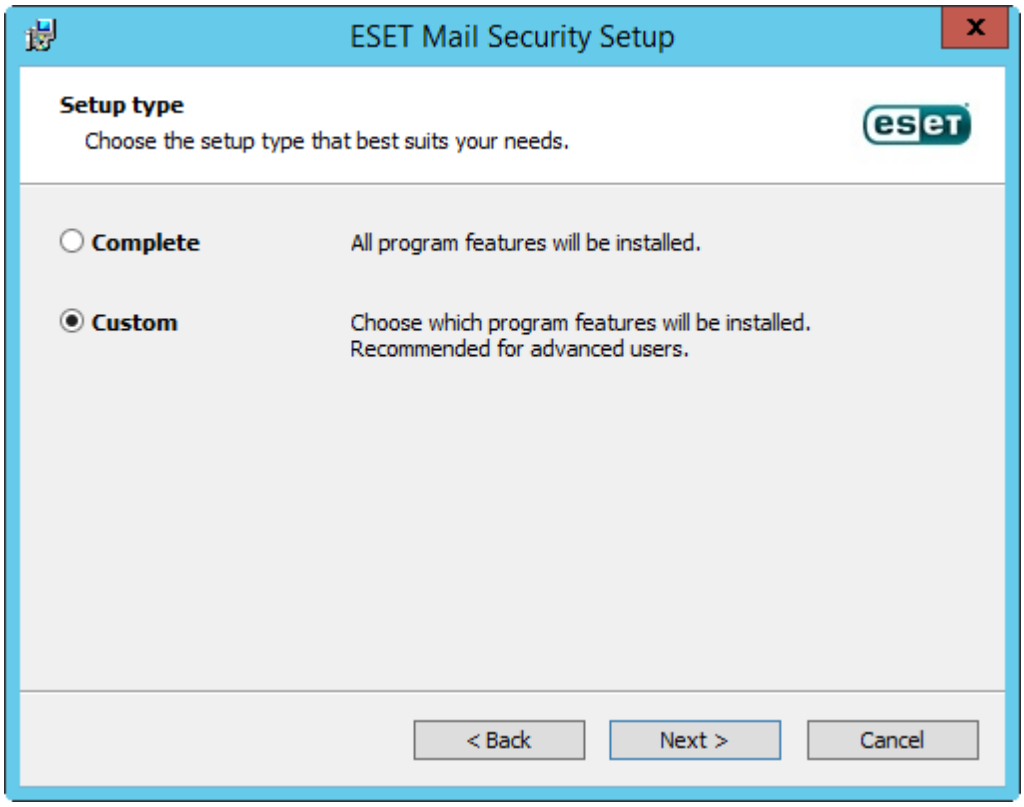
NOTE: On Windows Server 2008 and Windows Server 2008 R2, installation of **Web and email** component is disabled by default. If you want to have this component installed, choose **Custom** installation type.

NOTE: In case you are planning to use Local quarantine for email messages and do not want to have quarantined message files stored on your `C:` drive, change the path of **Data folder** to your preferred drive and location. However, keep in mind that all ESET Mail Security data files will be stored in this location.



Custom installation:

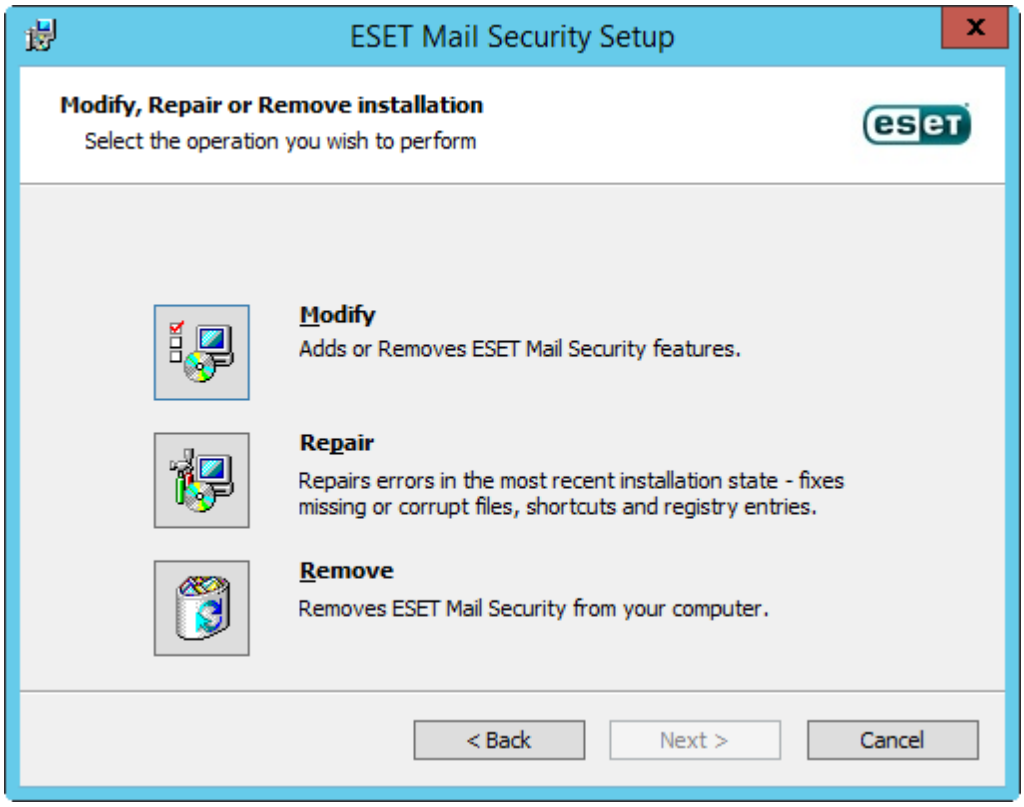
Lets you choose which features you want to install. Useful when you want to customize ESET Mail Security with only the components you need.



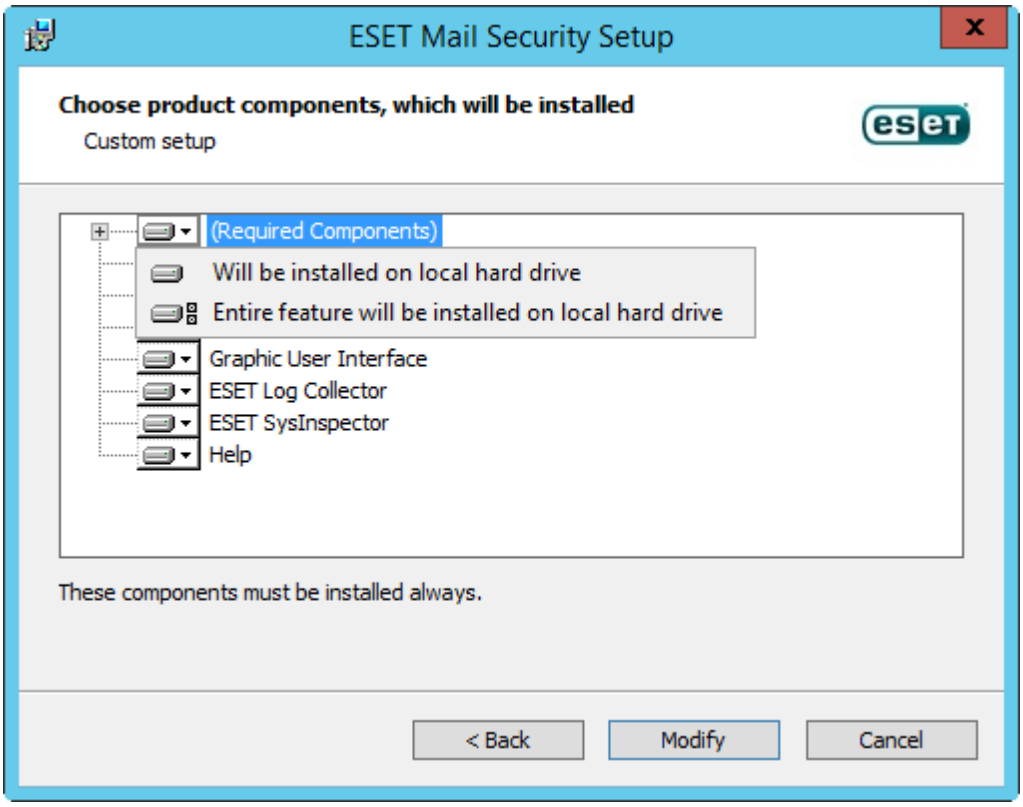
You can add or remove components included in your installation. To do so, run the .msi installer package you used during initial installation, or go to **Programs and Features** (accessible from the Windows Control Panel), right-click ESET Mail Security and select **Change**. Follow the steps below to add or remove components.

Component modification (Add/Remove) process, Repair and Remove:

There are 3 options available. You can **Modify** installed components, **Repair** your installation of ESET Mail Security or **Remove** (uninstall) it completely.


ESET Mail Security Setup
Modify, Repair or Remove installation
Select the operation you wish to perform
Modify
Adds or Removes ESET Mail Security features.
Repair
Repairs errors in the most recent installation state - fixes missing or corrupt files, shortcuts and registry entries.
Remove
Removes ESET Mail Security from your computer.
< Back
Next >
Cancel

If you choose **Modify,** a list of available program components is displayed. Choose the components you want to add or remove. You can add/remove multiple components at the same time. Click the component and select an option from the drop-down menu:



When you have selected an option, click **Modify** to perform the modifications.

NOTE: You can modify installed components at any time by running the installer. For most components, a server restart is not necessary to carry out the change. The GUI will restart and you'll only see only the components you chose to install. For components that require a server restart, the Windows Installer will prompt you to restart and new components will become available once the server is back online.

3.1.1 Command line installation

The following settings are intended for use **only with the reduced**, **basic and none** level of the user interface. See documentation for the **msiexec** version used for the appropriate command line switches.

Supported parameters:

APPDIR=<path>
- path - Valid directory path
- Application installation directory.
- For example: `emsx_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>
- path - Valid directory path
- Application Data installation directory.

MODULEDIR=<path>
- path - Valid directory path
- Module installation directory.

ADDEXCLUDE=<list>

- The ADDEXCLUDE list is a comma-separated list of all feature names not to be installed, as a replacement for the obsolete REMOVE.
- When selecting a feature not to install, then the whole path (i.e., all its sub-features) and related invisible features must be explicitly included in the list.
- For example: `ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network`

NOTE: The **ADDEXCLUDE** cannot be used together with **ADDLOCAL**.

ADDLOCAL=<list>

- Component installation - list of non-mandatory features to be installed locally.
- Usage with ESET .msi packages: `emsx_nt64_ENU.msi /qn ADDLOCAL=<list>`
- For more information about the **ADDLOCAL** property see http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

Rules

- The **ADDLOCAL list** is a comma separated list of all feature names to be installed.
- When selecting a feature to install, the whole path (all parent features) must be explicitly included in the list.
- See additional rules for correct usage.

Feature Presence

- **Mandatory** - the feature will be always installed
- **Optional** - the feature may be deselected for install
- **Invisible** - logical feature mandatory for other features to work properly
- **Placeholder** - feature with no effect on the product, but must be listed with sub-features

Feature tree is following:

Feature tree	Feature Name	Feature Presence
Computer	Computer	Mandatory
Computer / Antivirus and antispyware	Antivirus	Mandatory
Computer / Antivirus and antispyware > Real-time file system protection	RealtimeProtection	Mandatory
Computer / Antivirus and antispyware > Computer scan	Scan	Mandatory
Computer / Antivirus and antispyware > Document protection	DocumentProtection	Optional
Computer / Device control	DeviceControl	Optional
Network	Network	Placeholder
Network / Personal Firewall	Firewall	Optional
Web and e-mail	WebAndEmail	Placeholder
Web and e-mail ProtocolFiltering	ProtocolFiltering	Invisible
Web and e-mail / Web access protection	WebAccessProtection	Optional
Web and e-mail / E-mail client protection	EmailClientProtection	Optional
Web and e-mail / E-mail client protection / MailPlugins	MailPlugins	Invisible
Web and e-mail / E-mail client protection / Antispam protection	Antispam	Optional
Web and e-mail / Web control	WebControl	Optional
Update mirror	UpdateMirror	Optional
Microsoft NAP support	MicrosoftNAP	Optional

Additional rules

- If any of the **WebAndEmail** feature/s is selected to be installed, the invisible **ProtocolFiltering** feature must be explicitly included in the list.
- If any of the **EmailClientProtection** sub-features/s is selected to be installed, the invisible **MailPlugins** feature must be explicitly included in the list

Examples:

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

List of CFG_ properties:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 - Disabled, 1 - Enabled

CFG_LIVEGRID_ENABLED=1/0
• 0 - Disabled, 1 - Enabled
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 - Disable, 1 - Enable
• Schedule a new FirstScan after installation.

CFG_EPFW_MODE=0/1/2/3
• 0 - Automatic, 1 - Interactive, 2 - Policy, 3 - Learning

CFG_PROXY_ENABLED=0/1
• 0 - Disabled, 1 - Enabled

CFG_PROXY_ADDRESS=<ip>
• Proxy IP address.

CFG_PROXY_PORT=<port>
• Proxy port number.

CFG_PROXY_USERNAME=<user>
• User name for authentication.

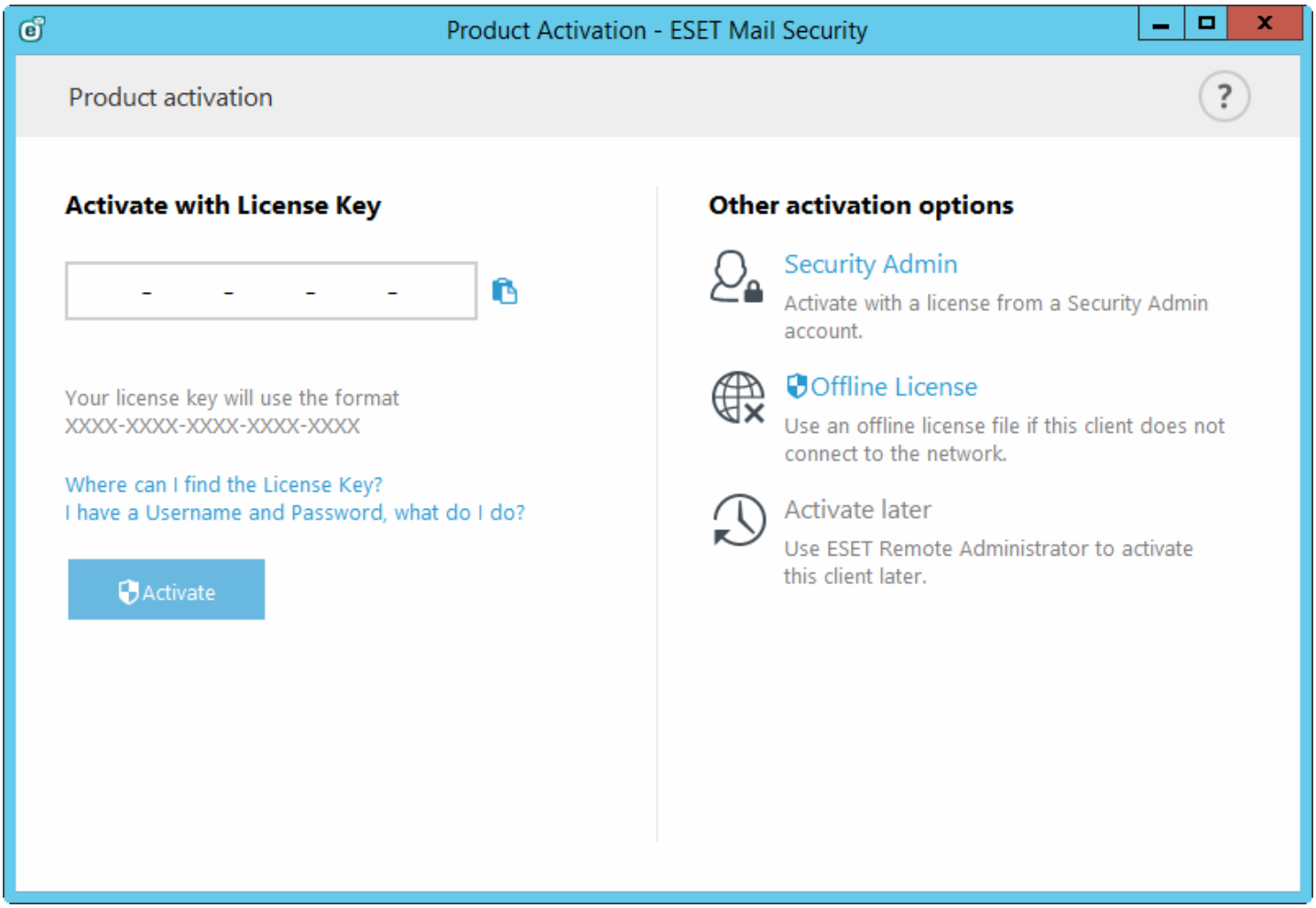
CFG_PROXY_PASSWORD=<pass>
• Password for authentication.

3.1.2 Installation in cluster environment

You can deploy ESET Mail Security in a cluster environment (for example failover cluster). We recommend you to install ESET Mail Security on an active node and then redistribute the installation on passive node(s) using ESET Cluster feature of ESET Mail Security. Apart from the installation, ESET Cluster will serve as replication of ESET Mail Security configuration to ensures consistency between cluster nodes necessary for correct operation.

3.2 Product activation

When installation is complete, you will be prompted to activate your product.


Product Activation - ESET Mail Security
Product activation
Activate with License Key
Your license key will use the format
XXXX-XXXX-XXXX-XXXX-XXXX
Where can I find the License Key?
I have a Username and Password, what do I do?
Activate
Other activation options
Security Admin
Activate with a license from a Security Admin account.
Offline License
Use an offline license file if this client does not connect to the network.
Activate later
Use ESET Remote Administrator to activate this client later.

Select one of the available methods to activate ESET Mail Security. See How to activate ESET Mail Security for more information.

After you've successfully activated ESET Mail Security, the main program window will open and display your current status in the Monitoring page.

The main program window will also display notifications about other items, such as system updates (Windows Updates) or virus signature database updates. When all items that require attention are resolved, the monitoring status will turn green and display the status "**Maximum protection**".

3.3 Terminal Server

If you are installing ESET Mail Security on a Windows Server that acts as a Terminal Server, you may want to disable the ESET Mail Security GUI to prevent it from starting up every time a user logs in. See Disable GUI on Terminal Server for specific steps to disable the GUI.

3.4 ESET AV Remover

To remove/uninstall third-party antivirus software from your system, we recommend that you use the ESET AV Remover. To do so, follow these steps:

1. Download the ESET AV Remover from ESET website Utilities download page.
2. Click **I accept, start search** to accept the EULA and begin searching your system.
3. Click **Launch uninstaller** to remove the installed antivirus software.

For a list of third-party antivirus software that can be removed using ESET AV Remover see this KB article.

3.5 Upgrading to a newer version

New versions of ESET Mail Security are issued to provide improvements or fix issues that cannot be resolved by automatic updates to program modules. It is possible to perform an upgrade from older versions of ESET Mail Security (4.5 and earlier) even though it is an upgrade to a different architecture. You can upgrade to a newer version:

- Manually, by downloading and installing a more recent version over your existing version. Simply run the installer and perform an installation as usual, ESET Mail Security will transfer your existing configuration automatically, however with some exceptions (see the note below).

IMPORTANT: There are some exceptions during upgrade, not all of your settings will be preserved, in particular Rules. This is due to the Rules functionality being completely redesigned in ESET Mail Security 6. Rules in previous versions of ESET Mail Security are not compatible with Rules in ESET Mail Security version 6. We recommend you to configure Rules manually by defining email filtering conditions and actions to take with filtered emails. New Rules gives you greater flexibility and even more possibilities compared to Rules in previous version of ESET Mail Security.

Following is a list of settings that are preserved from previous versions of ESET Mail Security:

- General ESET Mail Security configuration.
- Antispam protection settings:
  - All settings that are identical in previous versions, any new settings will use defaults.
  - Whitelists and blacklists.

NOTE: Once you've upgraded your ESET Mail Security, we recommend you to go through all the settings to make sure it is configured correctly and according to your needs.

3.6 Exchange Server Roles - Edge vs Hub

Both Edge Transport and Hub Transport Servers have antispam features disabled by default. This is the desired configuration in an Exchange organization with an Edge Transport server. We recommend that you have the Edge Transport server running ESET Mail Security antispam configured to filter messages before they are routed into the Exchange organization.

The Edge role is the preferred location for antispam scanning because it allows ESET Mail Security to reject spam early in the process without putting an unnecessary load on network layers. Using this configuration, incoming messages are filtered by ESET Mail Security on the Edge Transport server, so they can safely be moved to the Hub Transport server without the need for further filtering.

If your organization does not use an Edge Transport server and only has a Hub Transport server, we recommend that you enable antispam features on the Hub Transport server that receives inbound messages from the Internet via SMTP.

3.7 Exchange Server 2013 Roles

The architecture of Exchange Server 2013 is different from previous versions of Microsoft Exchange. Since the introduction of Exchange 2013, CU4 (which is in fact SP1 for Exchange 2013) has reintroduced the Edge Transport server role.

If you are planning to protect Microsoft Exchange 2013 with ESET Mail Security, make sure to install ESET Mail Security on a system running Microsoft Exchange 2013 with the Mailbox server or Edge Transport server role.

There is an exception if you are planning to install ESET Mail Security on Windows SBS (Small Business Server) or have Microsoft Exchange 2013 with multiple roles on a single server. In this case, all Exchange roles are running on the same server, thus ESET Mail Security will provide full protection including protection of mail servers.

If you install ESET Mail Security on a system running the Client Access server role only (dedicated CAS server), most important ESET Mail Security features will be disabled—especially mail server features. In this case, only real-time file system protection and some components that belong to Computer protection will be functional, so mail servers will not be protected. For this reason we do not recommend installing ESET Mail Security on a server with the Client Access server role. This does not apply to Windows SBS (Small Business Server) and Microsoft Exchange with multiple roles on the same computer as mentioned above.

NOTE: Due to the technical restrictions of Microsoft Exchange 2013, ESET Mail Security does not support the Client Access server (CAS) role. This does not apply to Windows SBS or Microsoft Exchange 2013 installed on a single server with all server roles—in this case you can run ESET Mail Security with the CAS role on the server since the Mailbox server and Edge Transport server are protected.

3.8 POP3 Connector and antispam

Microsoft Windows Small Business Server (SBS) versions contain native built-in POP3 Connector that enables the server to fetch email messages from external POP3 servers. Implementation of this Microsoft native POP3 Connector differs from one SBS version to another.

ESET Mail Security does support Microsoft SBS POP3 Connector, provided it is configured correctly. Messages downloaded via the Microsoft POP3 Connector are scanned for the presence of spam. Antispam protection for these messages is possible because the POP3 Connector forwards email messages from a POP3 account to Microsoft Exchange Server via SMTP.

ESET Mail Security has been tested with popular mail services such as **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** and **gmx.de** on the following SBS systems:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

IMPORTANT: If you are using built-in Microsoft SBS POP3 Connector and have all email messages scanned for spam, go to Advanced setup, navigate to **Server** > **Mail transport protection** > Advanced settings and for **Scan also messages received from authenticated or internal connections** setting choose **Scan by antivirus and antispam protection** from the drop-down list. This ensures antispam protection for email fetched from POP3 account(s).

You can also use a third party POP3 connector such as P3SS (instead of the built-in Microsoft SBS POP3 Connector). ESET Mail Security has been tested on the following systems (using P3SS connector fetching messages from **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** and **gmx.de**):

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 with Exchange Server 2007
- Microsoft Windows Server 2008 R2 with Exchange Server 2010
- Microsoft Windows Server 2012 R2 with Exchange Server 2013

4. Beginner's guide

This chapter provides an overview of ESET Mail Security, the main parts of the menu, functionalities and basic settings.

4.1 The user interface

The main program window of ESET Mail Security is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The different sections of the main menu are described below:

Monitoring - Provides information about the protection status of ESET Mail Security, license validity, last update of the virus signature database, basic statistics and system information.

Log files - Accesses log files that contain information about all important program events that have occurred. These files provide an overview of detected threats as well as other security related events.

Scan - Allows you to configure and launch a Storage scan, Smart scan, Custom scan or Removable media scan. You can also repeat the last scan that was run.

Mail Quarantine - Provides an easy management of quarantined emails. This Mail Quarantine manager is common for all three types - Local quarantine, Quarantine mailbox and MS Exchange quarantine.

Update - Displays information about the virus signature database and notifies you if an update is available. Product activation can also be performed from this section.

Setup - Here you can adjust your Server and Computer security settings.

Tools - Provides additional information about your system and protection in addition to tools that help you further manage your security. The Tools section contains the following items: Running processes, Watch activity, ESET Log Collector, Protection statistics, Cluster, ESET Shell, ESET SysInspector, ESET SysRescue Live to create a rescue CD or USB and Scheduler. You can also Submit sample for analysis and check your Quarantine.

Help and support - Provides access to help pages, the ESET Knowledgebase and other Support tools. Also available are links to open a Customer Care support request and information about product activation.

The protection status shown in the **Monitoring** section informs you about the current protection level of your computer. The green **Maximum protection** status indicates that maximum protection is ensured.

The status window also displays quick links to frequently used features in ESET Mail Security and information about the last update.

What to do if the program doesn't work properly?

Modules that are working properly are assigned a green check. Modules that are not fully functional are assigned a red exclamation point or an orange notification icon. Additional information about the module is shown in the upper part of the window. A suggested solution for fixing the module is also displayed. To change the status of an individual module, click **Setup** in the main menu and then click the desired module.

The red icon indicates critical problems - maximum protection of your computer is not ensured. This status is displayed when:

- **Antivirus and antispyware protection disabled** - You can re-enable antivirus and antispyware protection by clicking **Enable Real-time protection** in the **Protection status** pane or **Enable Antivirus and antispyware protection** in the **Setup** pane of the main program window.
- You are using an outdated virus signature database.
- The product is not activated.
- **Your license is expired** - This is indicated by the protection status icon turning red. The program is not able to update after the license expires. We recommend following the instructions in the alert window to renew your license.

The orange icon indicates that your ESET product requires attention for a non-critical problem. Possible reasons include:

- **Web access protection is disabled** - You can re-enable Web access protection by clicking the security notification and then clicking **Enable Web access protection**.
- **Your license will expire soon** - This is indicated by the protection status icon displaying an exclamation point. After your license expires, the program will not be able to update and the Protection status icon will turn red.

If you are unable to solve a problem using the suggested solutions, click **Help and support** to access the help files or search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Customer Care support request. ESET Customer Care will respond quickly to your questions and help find a resolution.

To view your **Protection status**, click the top option from the main menu. A status summary about the operation of ESET Mail Security will be displayed in the primary window, and a submenu with two items will appear: **Watch activity** and **Statistics**. Select either of these to view more detailed information about your system.

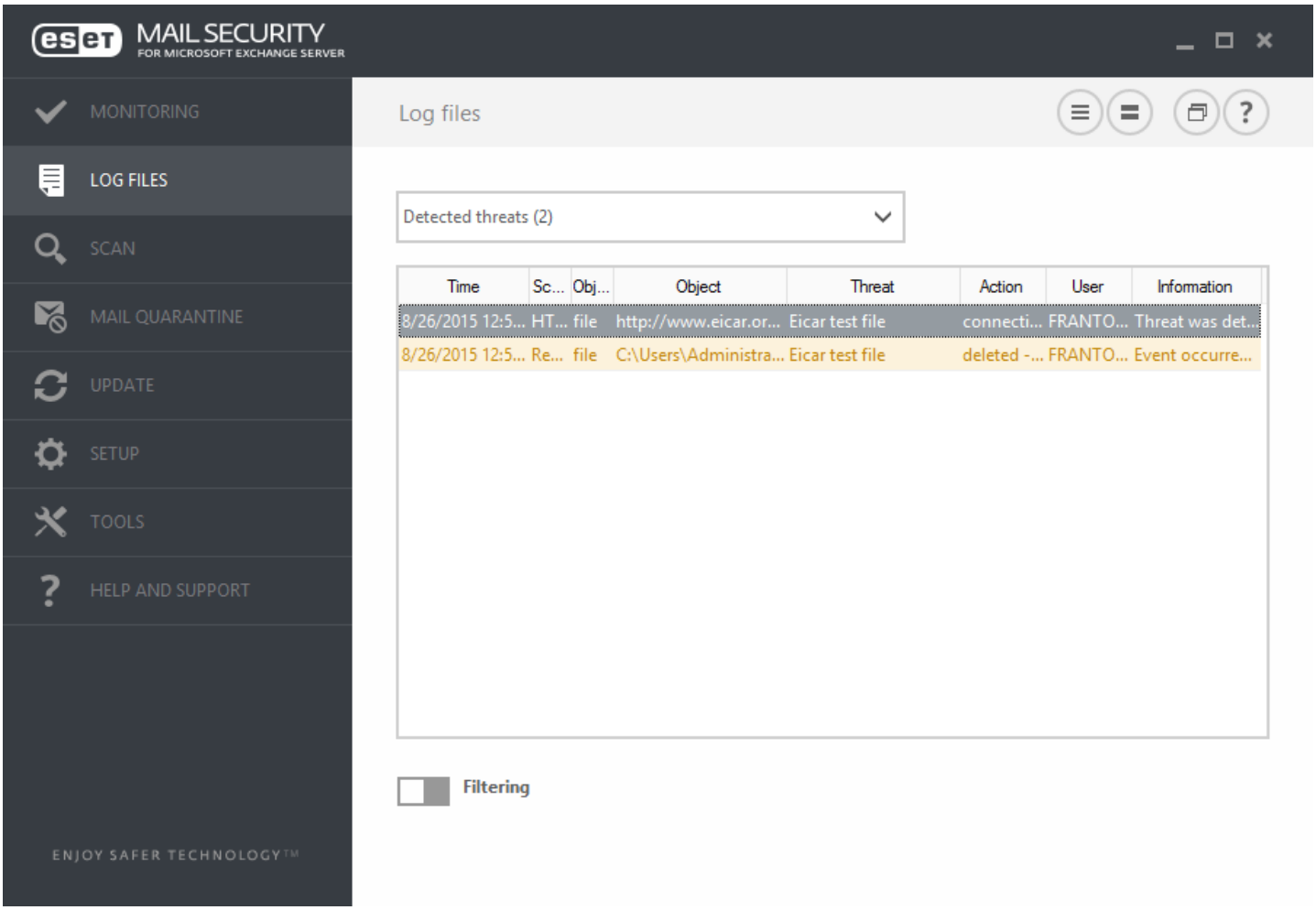
When ESET Mail Security runs with full functionality, the **Protection status icon** appears in green. When attention is required, it appears in orange or red.

Click **Watch activity** to view a real-time graph of file-system activity (horizontal axis). The vertical axis shows the amount of read data (blue line) and the amount of written data (red line).

The **Statistics** sub-menu allows you to see the number of infected, cleaned and clean objects for a particular module. There is a number of modules you can choose from by selecting from the drop-down list.

4.2 Log files

Log files contain information about important program events that have occurred and provide an overview of detected threats. Logs are essential for system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on log verbosity settings. It is possible to view text messages and logs directly from the ESET Mail Security environment or export them for viewing elsewhere.



Log files are accessible from the main program window by clicking **Log files**. Select the desired log type from the drop-down menu. The following logs are available:

- **Detected threats** - The threat log offers detailed information about infiltrations detected by ESET Mail Security modules. This includes the time of detection, name of infiltration, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window.
- **Events** - All important actions performed by ESET Mail Security are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed to help system administrators and users resolve problems. Often the information found here can help you find a solution for a problem occurring in the program.
- **Computer scan** - All scan results are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.
- **HIPS** - Contains records of specific rules that are marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the name of the rule created.
- **Filtered websites** - A list of websites that have been blocked by Web access protection. In these logs you can see the time, URL, user and application that opened a connection to the particular website.

- **Device control** - Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).
- **Database scan** - Contains the version of the virus signature database, date, scanned location, number of scanned objects, number of threats found, number of rule hits and time of completion.
- **Mail server protection -** All messages detected by ESET Mail Security as infiltration or as a spam are recorded here. These logs apply to following protection types: Antispam, Rules and Antivirus. When you double-click an item, a pop-up window will open with Additional information about detected email message, such as **IP address**, **HELO domain**, **Message ID**, **Scan type** showing the protection layer it was detected on. Also, you can see the result of Antivirus and Antispam scan and the reason why it was detected or whether a Rule was activated.
- **Greylisting** - All messages that have been evaluated using the greylisting method are recorded here.

In each section, the displayed information can be copied to the clipboard (keyboard shortcut **Ctrl** + **C**) by selecting the entry and clicking **Copy**. The **CTRL** and **SHIFT** keys can be used to select multiple entries.

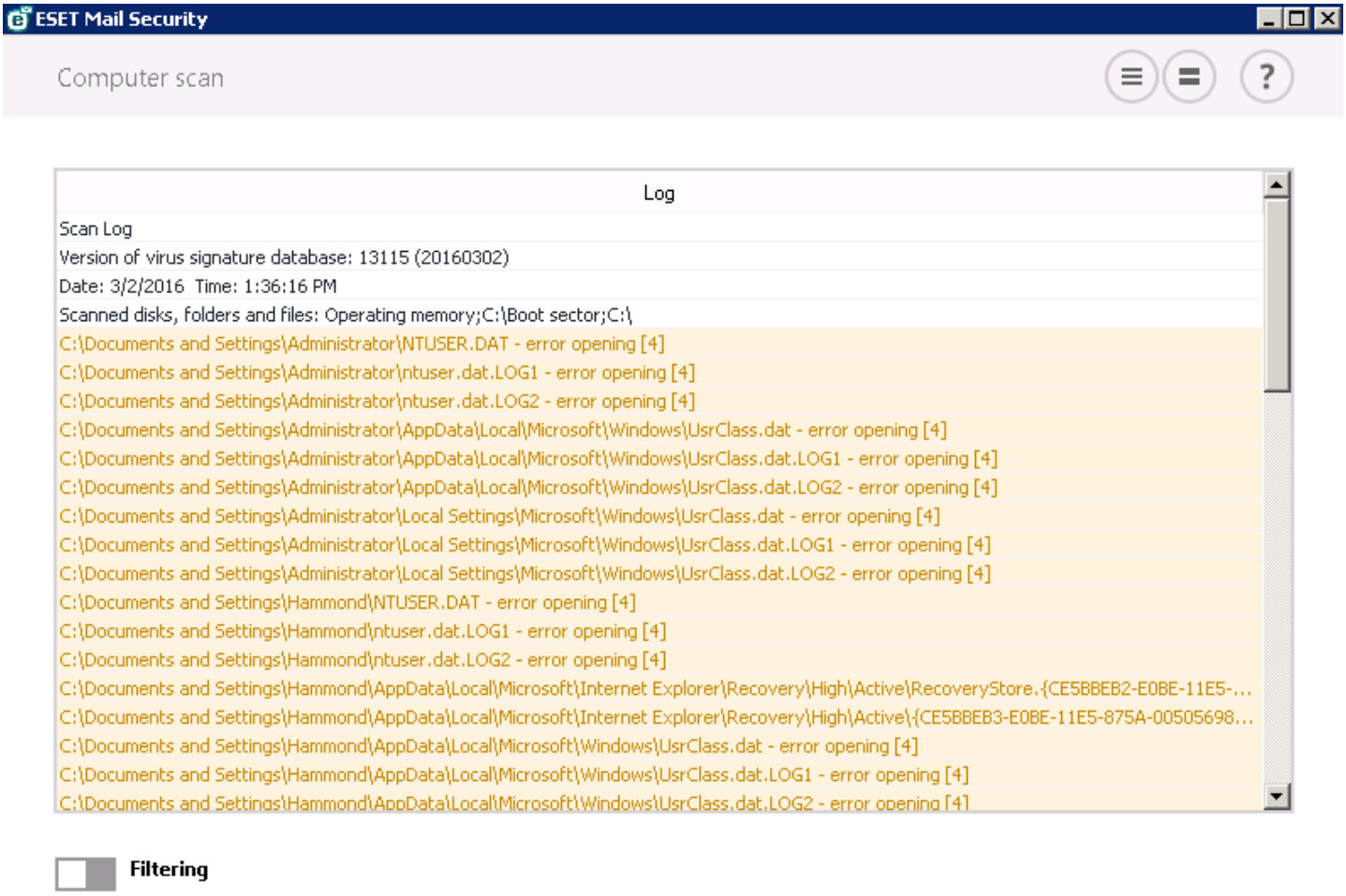
Click the switch icon **Filtering** to open the **Log filtering** window where you can define the filtering criteria.

You can bring up the context menu by right-clicking a specific record. The following options are available in the context menu:

- **Show** - Shows more detailed information about the selected log in a new window (same as double-click).
- **Filter same records** - This activates log filtering and only shows records of the same type as the one selected.
- **Filter...** - After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** - Activates filter settings. The first time that you filter logs, you must define your filtering criteria. Once filters are set they will remain unchanged until you edit them.
- **Disable filter** - Turns filtering off (same as clicking the switch at the bottom). This option is only available when filtering is turned on.
- **Copy** - Copies information from selected/highlighted record(s) to the clipboard.
- **Copy all** - Copies information of all the records in the window.
- **Delete** - Deletes selected/highlighted record(s) - this action requires administrator privileges.
- **Delete all** - Deletes all the record(s) in the window - this action requires administrator privileges.
- **Export...** - Exports information from a selected/highlighted record(s) into an XML file.
- **Export all...** - Exports all the information(s) in the window into an XML file.
- **Find...** - Opens the Find in log window and lets you define search criteria. Works on content that has already been filtered as an additional means of narrowing results.
- **Find next** - Finds the next occurrence of a previously defined search (above).
- **Find previous** - Finds the previous occurrence of a previously defined search (above).
- **Delete diagnostic records** - Deletes all diagnostic record(s) in the window.
- **Scroll log** - Leave this option enabled to auto scroll old logs and view active logs in the **Log files** window.

4.2.1 Scan log

The scan log window shows the current status of the scan and information about the number of files found that contain malicious code.


ESET Mail Security
Computer scan
Log
Scan Log
Version of virus signature database: 13115 (20160302)
Date: 3/2/2016 Time: 1:36:16 PM
Scanned disks, folders and files: Operating memory;C:\Boot sector;C:\
C:\Documents and Settings\Administrator\NTUSER.DAT - error opening [4]
C:\Documents and Settings\Administrator\ntuser.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\ntuser.dat.LOG2 - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
C:\Documents and Settings\Hammond\NTUSER.DAT - error opening [4]
C:\Documents and Settings\Hammond\ntuser.dat.LOG1 - error opening [4]
C:\Documents and Settings\Hammond\ntuser.dat.LOG2 - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CE5BBEB2-E0BE-11E5-...
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CE5BBEB3-E0BE-11E5-875A-00505698...
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
Filtering

In each section, the displayed information can be copied to the clipboard (keyboard shortcut **Ctrl** + **C**) by selecting the entry and clicking **Copy**. The **CTRL** and **SHIFT** keys can be used to select multiple entries.

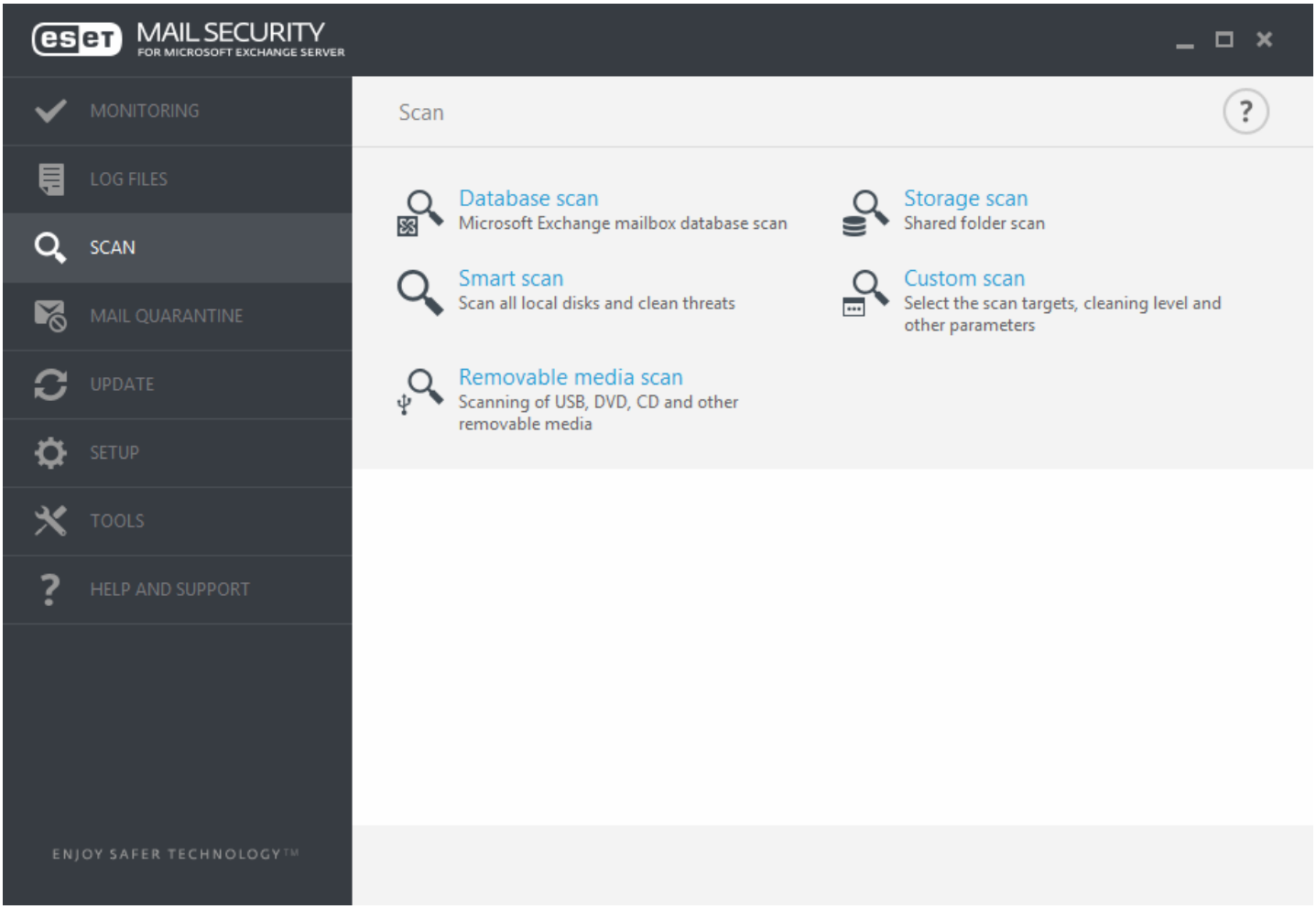
Click the switch icon **Filtering** to open the **Log filtering** window where you can define the filtering criteria.

You can bring up the context menu by right-clicking a specific record. The following options are available in the context menu:

- **Filter same records** - This activates log filtering and only shows records of the same type as the one selected.
- **Filter...** - After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** - Activates filter settings. The first time that you filter logs, you must define your filtering criteria. Once filters are set they will remain unchanged until you edit them.
- **Disable filter** - Turns filtering off (same as clicking the switch at the bottom). This option is only available when filtering is turned on.
- **Copy** - Copies information from selected/highlighted record(s) to the clipboard.
- **Copy all** - Copies information of all the records in the window.
- **Export...** - Exports information from a selected/highlighted record(s) into an XML file.
- **Export all...** - Exports all the information(s) in the window into an XML file.
- **Find...** - Opens the Find in log window and lets you define search criteria. Works on content that has already been filtered as an additional means of narrowing results.
- **Find next** - Finds the next occurrence of a previously defined search (above).
- **Find previous** - Finds the previous occurrence of a previously defined search (above).

4.3 Scan

The on-demand scanner is an important part of ESET Mail Security. It is used to perform scans of files and folders on your computer. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular (for example once a month) in-depth scans of your system to detect viruses not detected by Real-time file system protection. This can happen if Real-time file system protection was disabled at the time, if the virus database was obsolete or if the file was not detected as a virus when it was saved to the disk.



Two types of **Computer scan** are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** allows you to select any of the predefined scan profiles and define specific scan targets.

See Scan progress for more information about the scanning process.

Database scan

Lets you run On-demand database scan. You can choose **Public folders, Mail Servers and Mailboxes** to scan. Also, you can use Scheduler to run the database scan at a specific time or at an event.

NOTE: If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Mailbox database protection and On-demand database scan. However, only one protection type out of these two can be active at a time. If you decide to use On-demand database scan you'll need to disable integration of Mailbox database protection in Advanced setup under Server. Otherwise On-demand **database scan** will not be available.

Storage scan

Scans all shared folders on the local server. If **Storage scan** is not available, it means there are no shared folders on your server.

Hyper-V scan

This option is visible in the menu only if Hyper-V Manager is installed on the server that runs ESET Mail Security. Hyper-V scan allows for scanning of Virtual Machine (VM) disks on Microsoft Hyper-V Server without the need to have any "Agent" installed on the particular VM. See Hyper-V scan for more information (including list supported host operating systems and limitations).

Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is that it is easy to operate and does not require detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see Cleaning.

Custom scan

Custom scan is an optimal solution if you want to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed using the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and select an option from the **Scan targets** drop-down menu, or select specific targets from the tree structure. A scan target can also be specified by entering the path of the folder or file(s) you want to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. When performing a scan, you can choose from three cleaning levels by clicking **Setup** > **ThreatSense parameters** > **Cleaning**.

Performing computer scans with Custom scan is only recommended for advanced users with previous experience using antivirus programs.

Removable media scan

Similar to Smart scan - quickly launch a scan of removable media (such as CD/DVD/USB) that are connected to the computer. This may be useful when you connect a USB flash drive to a computer and want to scan its content for malware and other potential threats.

This type of scan can be also initiated by clicking **Custom scan** and then selecting **Removable media** from the **Scan targets** drop-down menu and clicking **Scan**.

Repeat last scan

Runs the last scan, whichever it was (Storage, Smart, Custom, etc.), with the exact same settings.

NOTE: Repeat last scan function is not available if On-demand database scan is present.

NOTE: We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.

4.3.1 Hyper-V scan

Hyper-V antivirus scan provides the ability to scan the disks of a Microsoft Hyper-V Server, that is, Virtual Machine (VM) without the need to have any Agent installed on the particular VM. The anti-virus is installed using the privileges of Administrator of the Hyper-V server.

Hyper-V scan is derived from the On-Demand computer scan module, while some features were not implemented (scan of Operating Memory).

Supported Host Operating Systems

- Windows Server 2008 R2 - Virtual Machines can be scanned only while they are offline
- Windows Server 2012
- Windows Server 2012 R2

Hardware requirements

The server should have no performance issues running Virtual Machines. The scan itself uses mostly only the resources of CPU.
In case of scanning online VM's free disk space is required. The free (available to use) disk space must be at least the double of the space used by checkpoints/snapshots and virtual disks.

Specific limitations

- Scanning on RAID storage, Spanned Volumes and Dynamic Disks is not supported due to the nature of Dynamic Disks. Therefore, we recommend you to avoid using Dynamic Disk type in your VM's if possible.
- Scanning is always performed on current Virtual Machine only, it does not affect its checkpoints/snapshots.
- Hyper-V running on a host in a cluster is currently not supported by ESET Mail Security.
- Virtual Machines on a Hyper-V host running on Windows Server 2008 R2 can only be scanned in read-only mode (**No cleaning**), regardless of what Cleaning level is selected in ThreatSense parameters.

NOTE: ESET Mail Security supports scanning of virtual disk MBR, however this is read-only scan. Scanning of MBR is being preformed by default. This setting can be changed in **Advanced setup** > **Antivirus** > **Hyper-V scan** > ThreatSense parameters > **Boot sectors**.

Virtual Machine to be scanned is "offline" - switched **Off** state

ESET Mail Security uses Hyper-V Management to detect and to connect to virtual disks of Virtual Machines. This way, ESET Mail Security has the same access to the content of the virtual disks as if accessing the data and files of any generic drive.

Virtual Machine to be scanned is "online" - **Running**, **Paused**, **Saved** state

ESET Mail Security uses Hyper-V Management to detect virtual disks of Virtual Machines. Actual connection to these the disks is not possible. Therefore, ESET Mail Security creates a checkpoint/snapshot of the Virtual Machine, then connects to the checkpoint/snapshot. Once the scan is completed, the checkpoint/snapshot is deleted. This meas that read-only scan can be performed because the Virtual Machine, that is online, remain unaffected. This is useful to obtain an overview whether there are infected items on running Virtual Machines and to get details about these infections, if there are any.

Creating a checkpoint/snapshot is a slow operation and might take from a few seconds to one minute. You should take this into account when planning to run Hyper-V scan on a larger amount of Virtual Machines.

Naming convention

The module of Hyper-V Scan sticks to the following naming convention:
`VirtualMachineName\DiskX\VolumeY`

where X is the number of disk and Y is the number of volume.
E.g.: `"Computer\Disk0\Volume1"`.

The number suffix is added based on the order of detection which is identical to the order seen in the Disk Manager of the VM.
This naming convention is used in the tree-structured list of targets to be scanned, in the progress bar and also in the log files.

Executing a scan

A scan can be executed 3 ways:

- On-demand - If you click the Hyper-V Scan option in the menu of ESET Mail Security, you will see a list of available Virtual Machines (if any) to be scanned. Its a tree-structured list where the lowest-level entity to be scanned is a volume, meaning, it is not possible to choose a directory or file to be scanned, but at least the entire volume has to be scanned.
  In order to list the available volumes we have to connect to the particular virtual disk(s) and this might take a few seconds. Therefore a faster option is to mark a Virtual Machine or its disk(s) to be scanned.
  Once you marked the desired Virtual Machines, disks or volumes to be scanned, click the Scan button.
- Via the scheduler
- Via ERA as a Client Task called Server Scan. The lowest-level item to be scanned is a disk of a Virtual Machine.

It is possible to execute several Hyper-V scans simultaneously.

Once the scan finishes, you see a notification about it and a Show log link by which you can review the details of accomplished scan. All the scan logs are available in the Log Files section of ESET Mail Security, but you have to choose Hyper-V scan from the drop-down menu in order to see the related logs.

Possible issues

- When executing the scan of an online Virtual Machine, a checkpoint/snapshot of the particular Virtual Machine has to be created and during the creation of a checkpoint/snapshot some generic actions of the Virtual Machine might be limited or disabled.
- If an offline Virtual Machine is being scanned, it cannot be turned on until the scan is finished.
- Hyper-V Manager allows to name two different Virtual Machines identically and this presents an issue when trying to differentiate the machines while reviewing the scan logs.

4.4 Mail Quarantine

The Mail Quarantine manager is available for all three Quarantine types:

- Local quarantine
- Quarantine mailbox
- MS Exchange quarantine

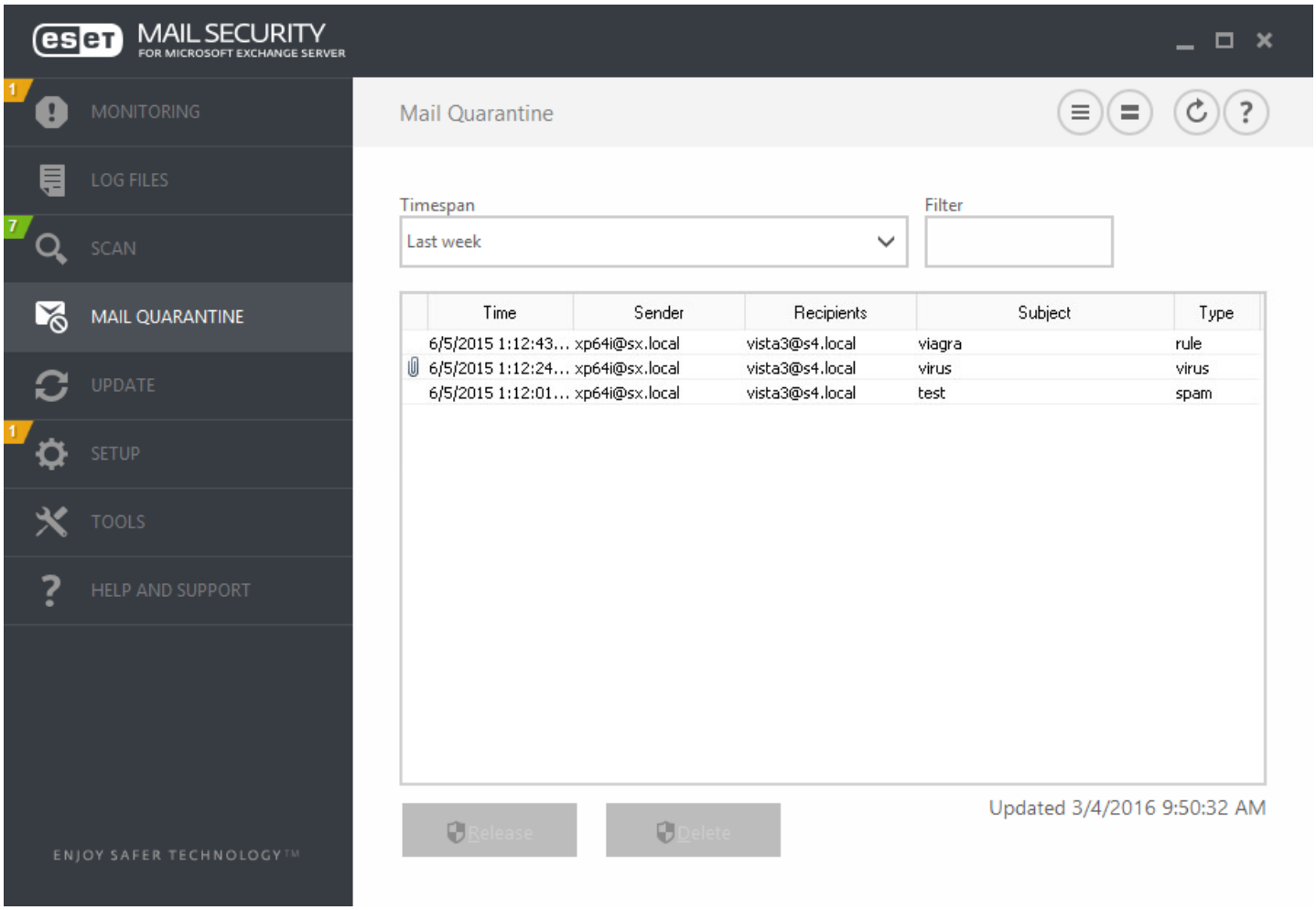
NOTE: If your Mail Quarantine manager is grayed out, it is because of the following reasons. You are running Microsoft Exchange Server 2003 on which this feature is not supported, or EWS (Exchange Web Services) is not available. This does not applies to Local quarantine, Local quarantine will work on all Exchange Servers and regardless of EWS availability.

NOTE: The Mail Quarantine Web interface is an alternative to Mail Quarantine manager that allows you to manage quarantined email objects.

Filtering

- **Timespan** - you can select the Timespan from which emails are displayed (1 week by default). When you change the Timespan, Mail Quarantine items are automatically reloaded.
- **Filter** - you can use filtering text box to filter displayed emails (all columns are searched).

NOTE: Mail Quarantine manager data is not updated automatically, we recommend that you click **refresh** regularly to see the most current items in the Mail Quarantine.

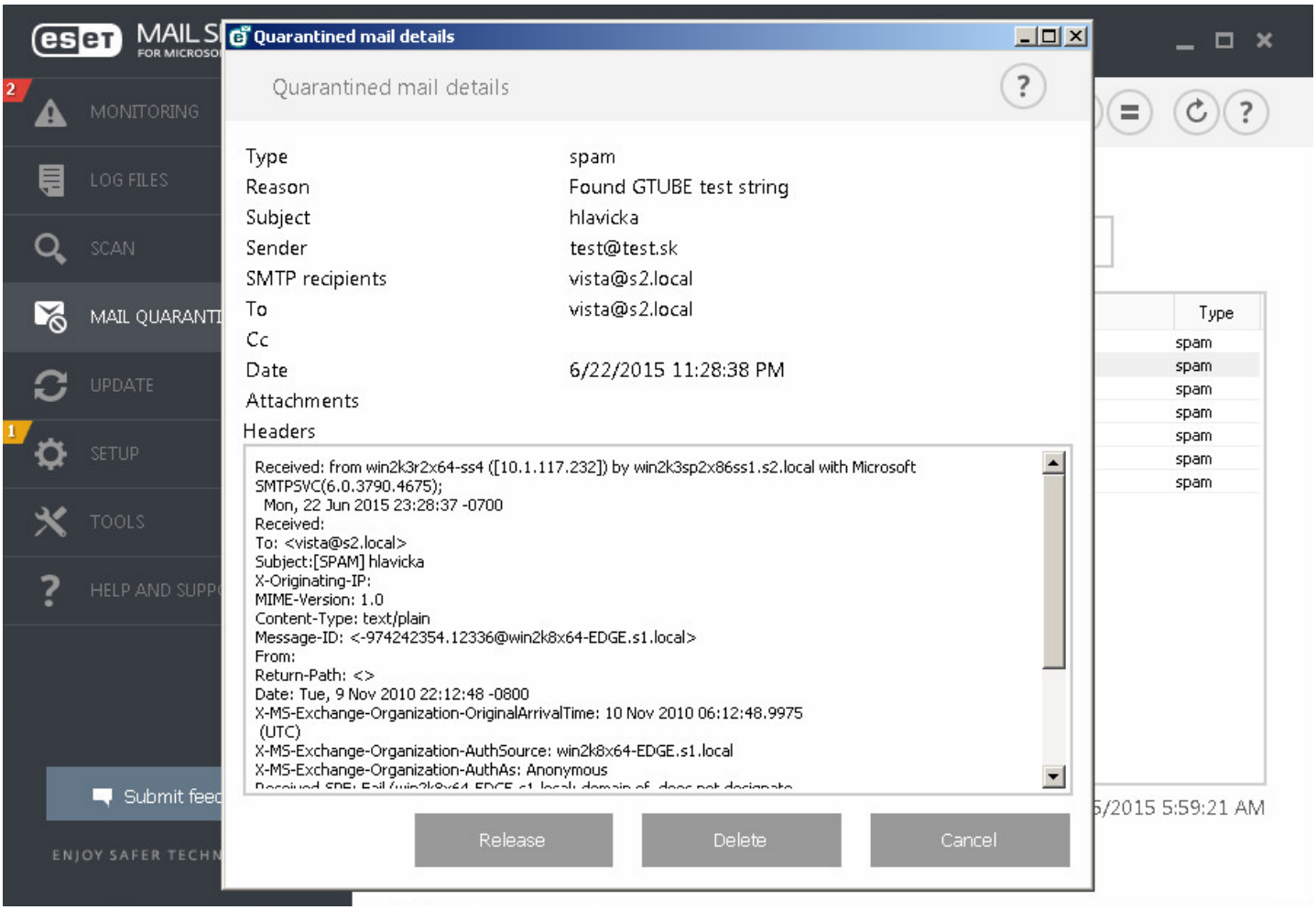


Action

- **Release** - releases email to its original recipient(s) using Replay directory and deletes it from quarantine. Click **Yes** to confirm the action.
- **Delete** - deletes item from quarantine. Click **Yes** to confirm the action.

Quarantine mail details - double click quarantined message or right-click and select **Details**, a pop-up window will open with details about the quarantined email message. You can also find some additional information about the email in the RFC email header.

Actions are also available from the context menu. If desired, click **Release**, **Delete** or **Delete permanently** to take an action with a quarantined email message. Click **Yes** to confirm the action. If you choose **Delete permanently** the message will be deleted from the file system as well, as opposed to **Delete** which will remove the item from Mail Quarantine manager view.



4.4.1 Quarantined mail details

This window contains information about the quarantined email message such as **Type**, **Reason**, **Subject**, **Sender**, **SMTP recipients**, **To**, **Cc**, **Date**, **Attachments** and **Headers**. You can select, copy and paste the headers if you need to.

You can take an action with the quarantined email message using buttons:

- **Release** - releases email to its original recipient(s) using Replay directory and deletes it from quarantine. Click **Yes** to confirm the action.
- **Delete** - deletes item from quarantine. Click **Yes** to confirm the action.

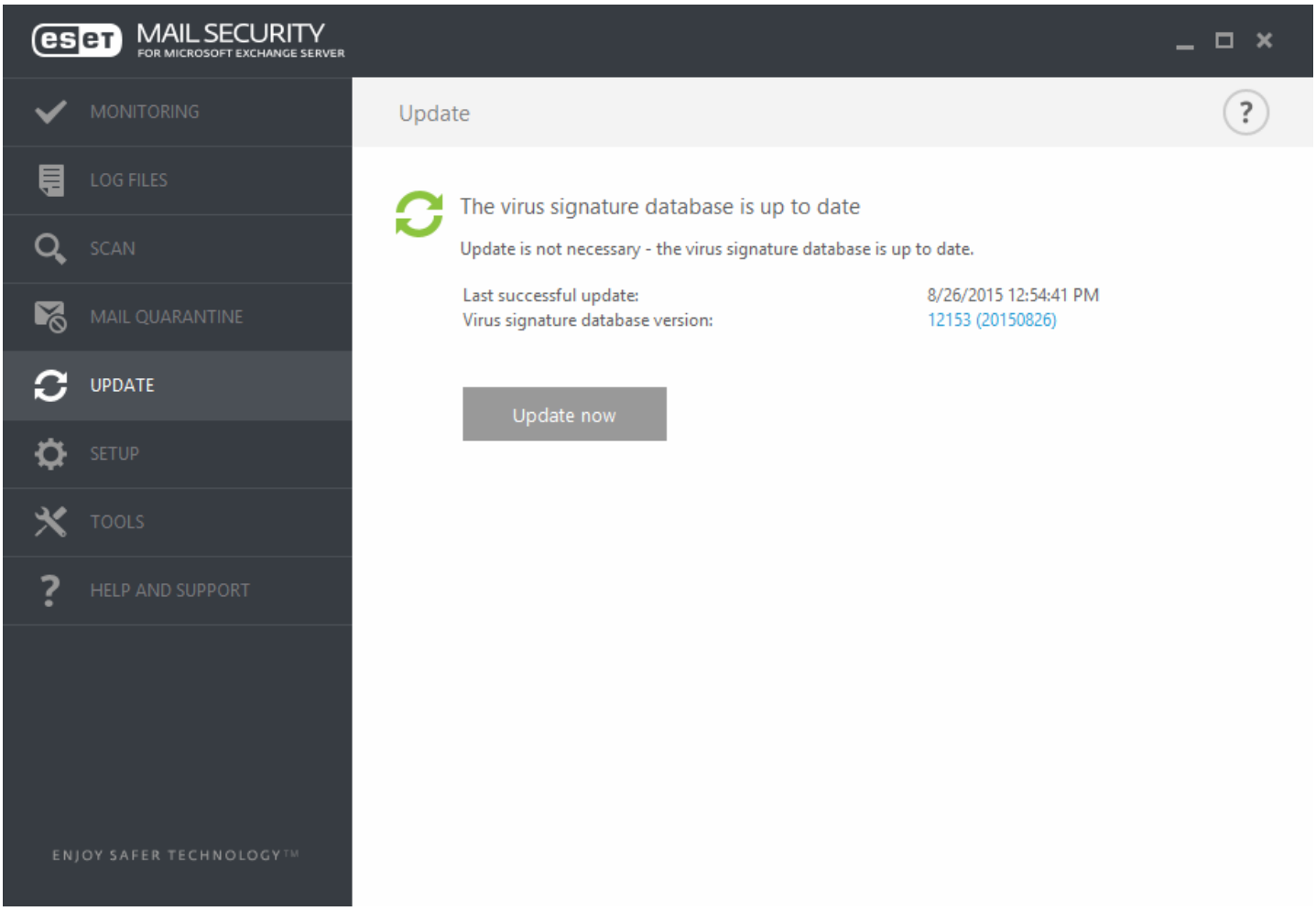
Clicking **Cancel** button will close Quarantined email details window.

4.5 Update

Regularly updating ESET Mail Security is the best method to maintain the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways, by updating the virus signature database and by updating system components.

By clicking **Update** in the main program window, you can find the current update status including the date and time of the last successful update and whether an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to the ESET website, listing all signatures added within the given update.

To begin the update process, click **Update now**. Updating the virus signature database and updating program components are important parts of maintaining complete protection against malicious code.



Last successful update - The date of the last update. Make sure it refers to a recent date, which means that the virus signature database is current.

Virus signature database version - The virus signature database number, which is also an active link to the ESET website. Click this to view a list of all signatures added in a given update.

Update process

After clicking **Update now**, the download process begins and the progress of the update is displayed. To interrupt the update click **Cancel update**.

IMPORTANT: Under normal circumstances, when updates are downloaded properly the message **Update is not necessary - the virus signature database is up to date** will appear in the **Update** window. If this is not the case, the program is out of date and more vulnerable to infection. Please update the virus signature database as soon as possible. Otherwise, one of the following messages will be displayed:

Virus signature database is out of date -This error will appear after several unsuccessful attempts to update the

virus signature database. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.

The previous notification is related to the following two **Virus signature database update failed** messages about unsuccessful updates:

Invalid license - The license key has been entered incorrectly in update setup. We recommend that you check your authentication data. The Advanced setup window (press **F5** on your keyboard) contains additional update options. Click **Help and support** > **Manage license** from the main menu to enter a new license key.

An error occurred while downloading update files - A possible cause of this error is incorrect Internet connection settings. We recommend that you check your Internet connectivity by opening any website in your web browser. If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.

NOTE: For more information please visit this ESET Knowledgebase article.

4.5.1 Setting up virus DB update

Updating the virus signature database and program components is an important part of providing complete protection against malicious code. Please pay careful attention to its configuration and operation. From the main menu, go to **Update** and then click **Update now** to check for a newer signature database.

You can configure update settings from the Advanced setup window (press the **F5** key on your keyboard). To configure advanced update options such as the update mode, proxy server access, LAN connection and virus signature copy settings (mirror), click **Update** in the **Advanced setup** window on the left. If you experience problems with an update, click **Clear cache** to clear the temporary update folder. The **Update server** menu is set to **AUTOSELECT** by default. **AUTOSELECT** means that the update server, from which the virus signature updates are downloaded, is chosen automatically. We recommend that you leave the default option selected. If you do not want the the system tray notification at the bottom right corner of the screen to appear, select **Disable display notification about successful update**.

For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct **License key** is entered in **Help and support** > **Activate License.**

If you did not activate your product following installation, you can do so at any time. For more detailed information about activation see How to activate ESET Mail Security and enter the license data you received with your ESET security product into the License details window.

4.5.2 Configuring Proxy server for updates

If you use a proxy server for the Internet connection on a system where ESET Mail Security is installed, proxy settings must be configured in Advanced setup. To access the proxy server configuration window, press **F5** to open the Advanced setup window and click **Update** > **HTTP proxy**. Select **Connection through a proxy server** from the **Proxy mode** drop-down menu and fill in your proxy server details: **Proxy server** (IP address), **Port** number and **Username** and **Password** (if applicable).

If you are unsure about proxy server details, you can try to automatically detect your proxy server settings by selecting **Use global proxy server settings** from the drop-down list.

NOTE: Proxy server options for various update profiles may differ. If this is the case, configure the different update profiles in Advanced setup by clicking **Update** > **Profile**.

4.6 Setup

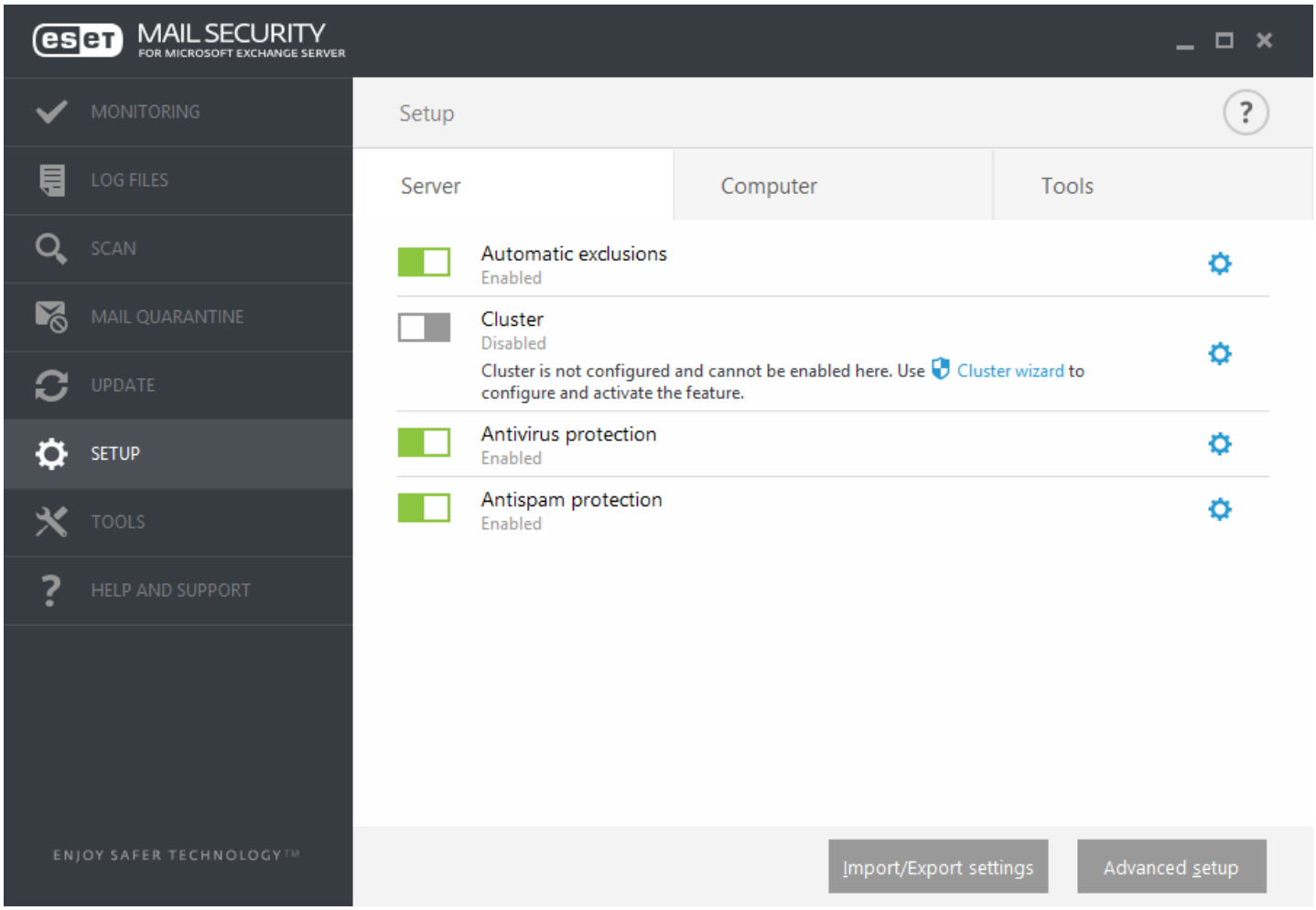
Setup menu consists of three tabs:

- Server
- Computer
- Tools

4.6.1 Server

ESET Mail Security provides protection for your server with essential functionalities such as: Antivirus and Antispyware, Resident shield (Real-time protection), Web-access protection and Email client protection. You can read more about each type of protection under the ESET Mail Security - Computer.

- Automatic exclusions feature identifies critical server applications and server operating system files and automatically adds them to the list of Exclusions. This functionality will minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.
- To setup the ESET Cluster click **Cluster wizard**. For details on how to set up the ESET Cluster using the wizard, click here.
- **Antivirus protection** - guards against malicious system attacks by controlling file, email and Internet communication.
- **Antispam protection** - integrates several technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting, etc.) to achieve maximum detection of email threats.



If you want to set more detailed options, click **Advanced setup** or press **F5**.

There are additional options at the bottom of the setup window. To load setup parameters using an *.xml*

configuration file, or to save the current setup parameters to a configuration file, use **Import/Export settings**. Please see Import/Export Settings for more detailed information.

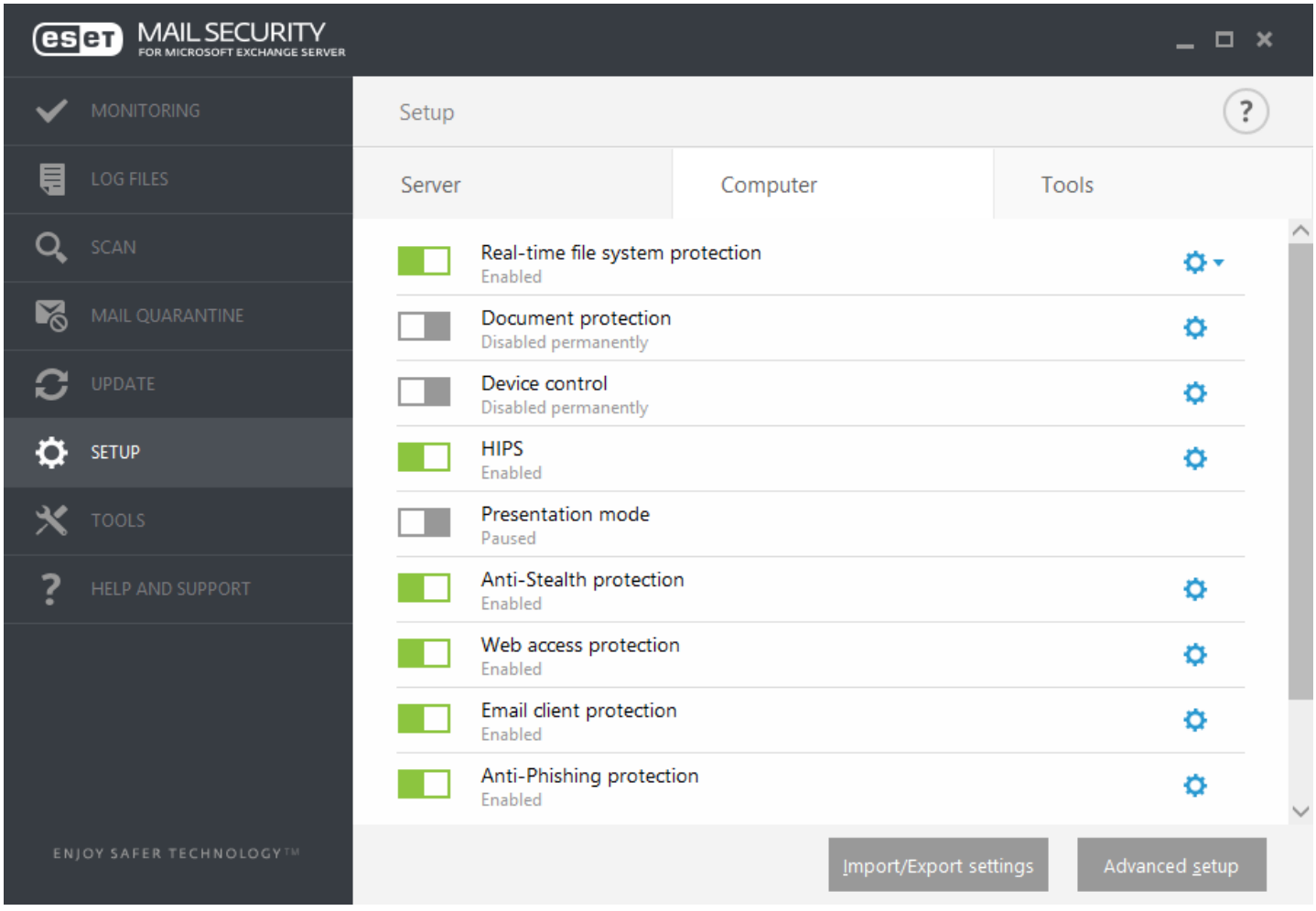
4.6.2 Computer

ESET Mail Security has all of the necessary components to ensure significant protection of the server as a computer. Each component provides a specific type of protection, such as: Antivirus and Antispyware, Real-time file system protection, Web-access, Email client, Anti-Phishing protection, etc.

The **Computer** section can be found under **Setup** > **Computer**. You'll see a list of components which you can enable/disable using the switch. To configure settings for a specific item, click the cogwheel. For **Real-time file system protection**, there is also an option to **Edit exclusions**, which will open the Exclusions setup window where you can exclude files and folders from scanning.

Pause Antivirus and antispyware protection - Any time that you temporarily disable Antivirus and antispyware protection, you can select the period of time for which you want the selected component to be disabled using the drop-down menu and then click **Apply** to disable the security component. To re-enable protection, click **Enable Antivirus and antispyware protection**.

The **Computer** module allows you to enable/disable and configure the following components:



- **Real-time file system protection** - All files are scanned for malicious code when they are opened, created or run on your computer.
- **Document protection** - The document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.
- **Device control -** This module allows you to scan, block or adjust extended filters/permissions and define a users ability to access and work with a given device.
- **HIPS** - The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.
- **Presentation mode** - A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.
- **Anti-Stealth protection** - Provides detection of dangerous programs, such as rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.
- **Web access protection** - If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** - Monitors communication received through the POP3 and IMAP protocol.
- **Anti-Phishing protection -** Protects you from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites disguised as legitimate ones.

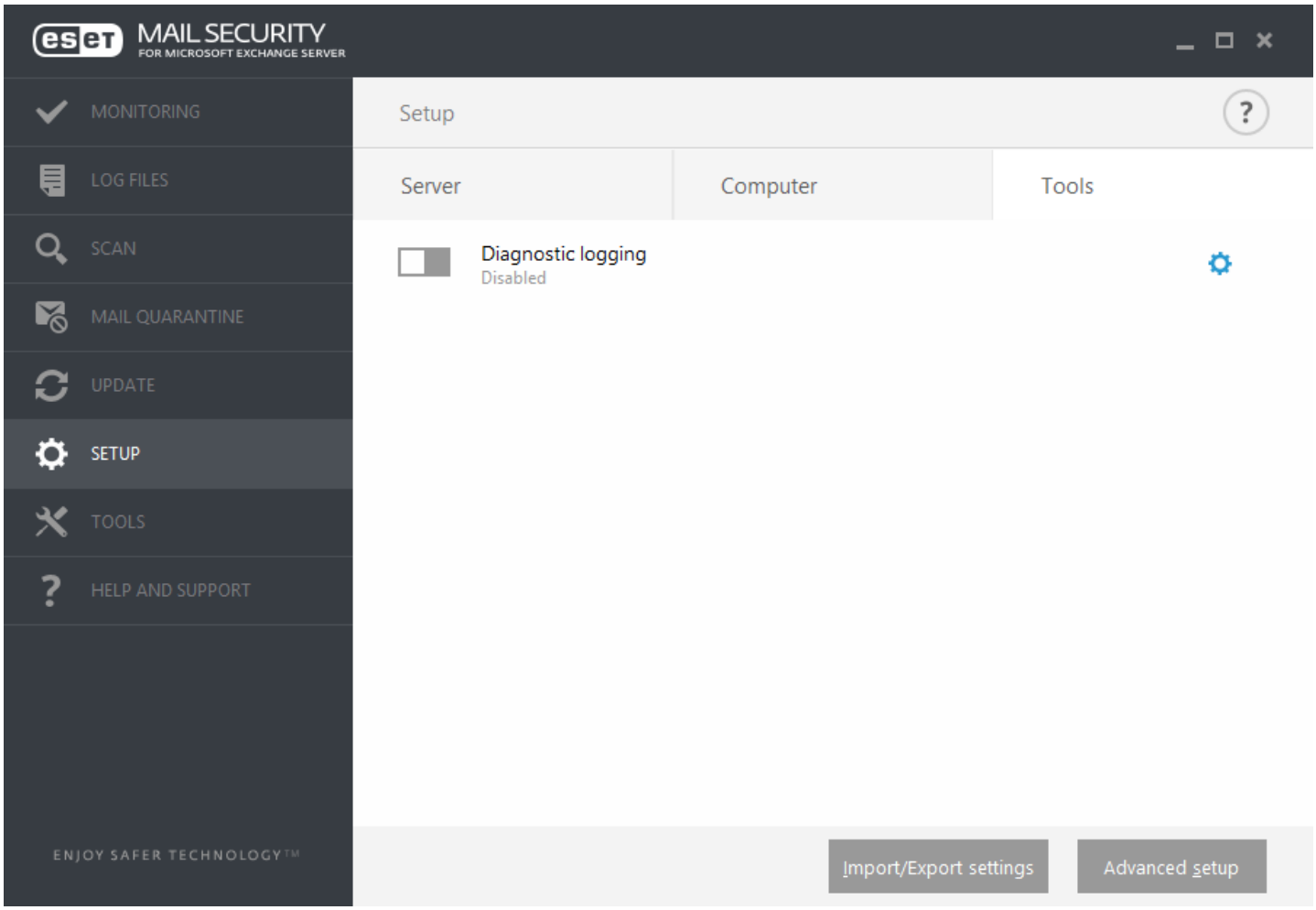
NOTE: Document protection is disabled by default. If you want, you can easily enable it by clicking the switch icon.

There are additional options at the bottom of the setup window. To load setup parameters using an *.xml* configuration file, or to save the current setup parameters to a configuration file, use **Import/Export settings**. Please see Import/Export settings for more detailed information.

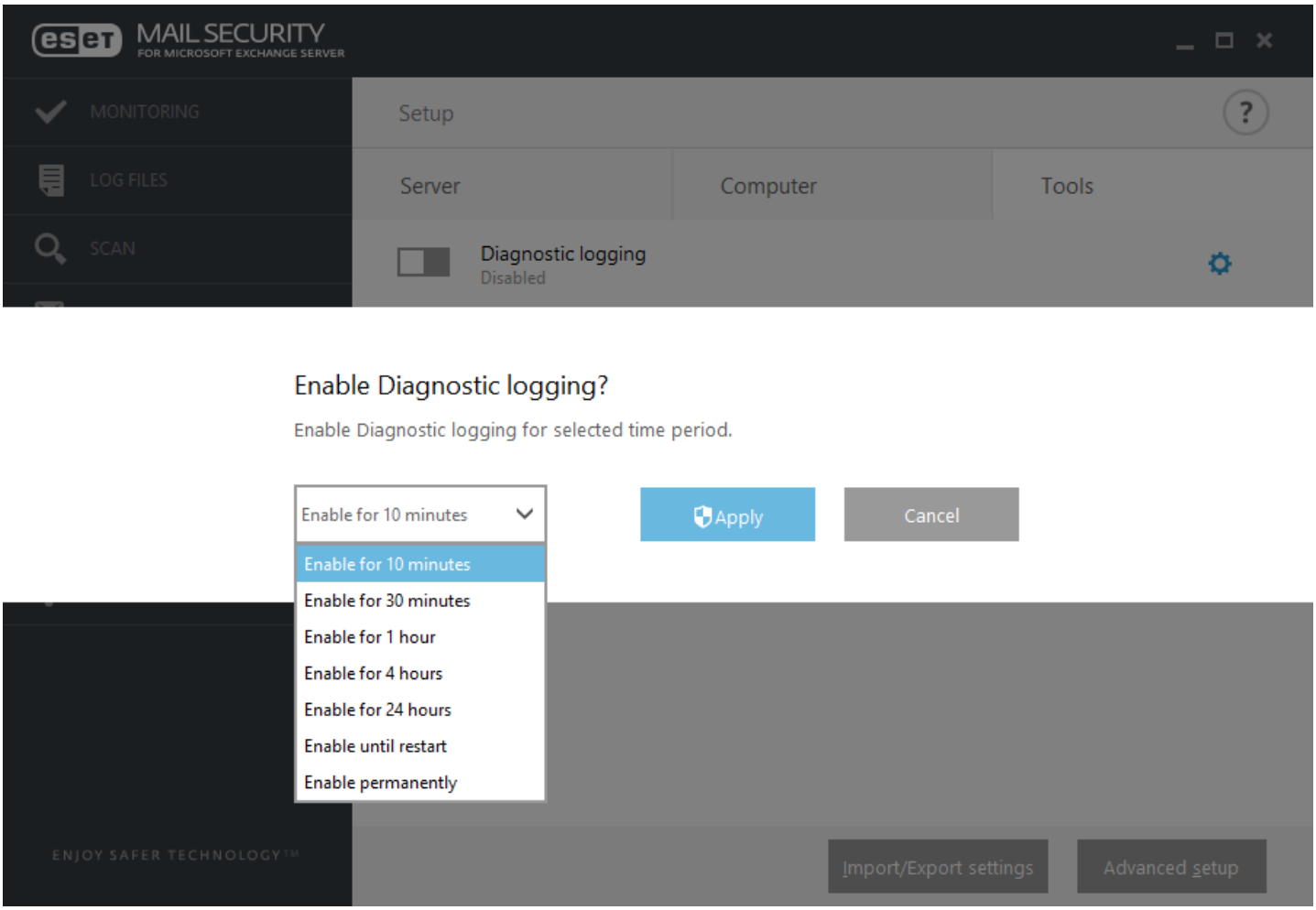
If you want to set more detailed options, click **Advanced setup** or press **F5**.

4.6.3 Tools

Diagnostic logging - configure witch components will write diagnostic logs when diagnostic logging is enabled. When you click the switch to enable diagnostic logging, you can choose for how long it will be enabled (10 minutes, 30 minutes, 1 hour, 4 hours, 24 hours, until next server restart or permanently). Components not shown in this tab always write diagnostic logs.



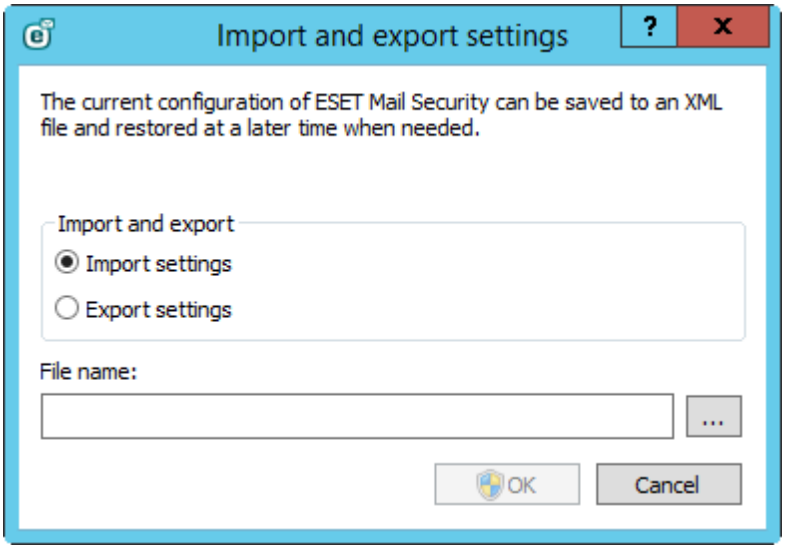
- **Enable** Diagnostic logging for selected time period.



4.6.4 Import and export settings

Importing and exporting the configuration of ESET Mail Security is available under **Setup** by clicking **Import/Export settings**.

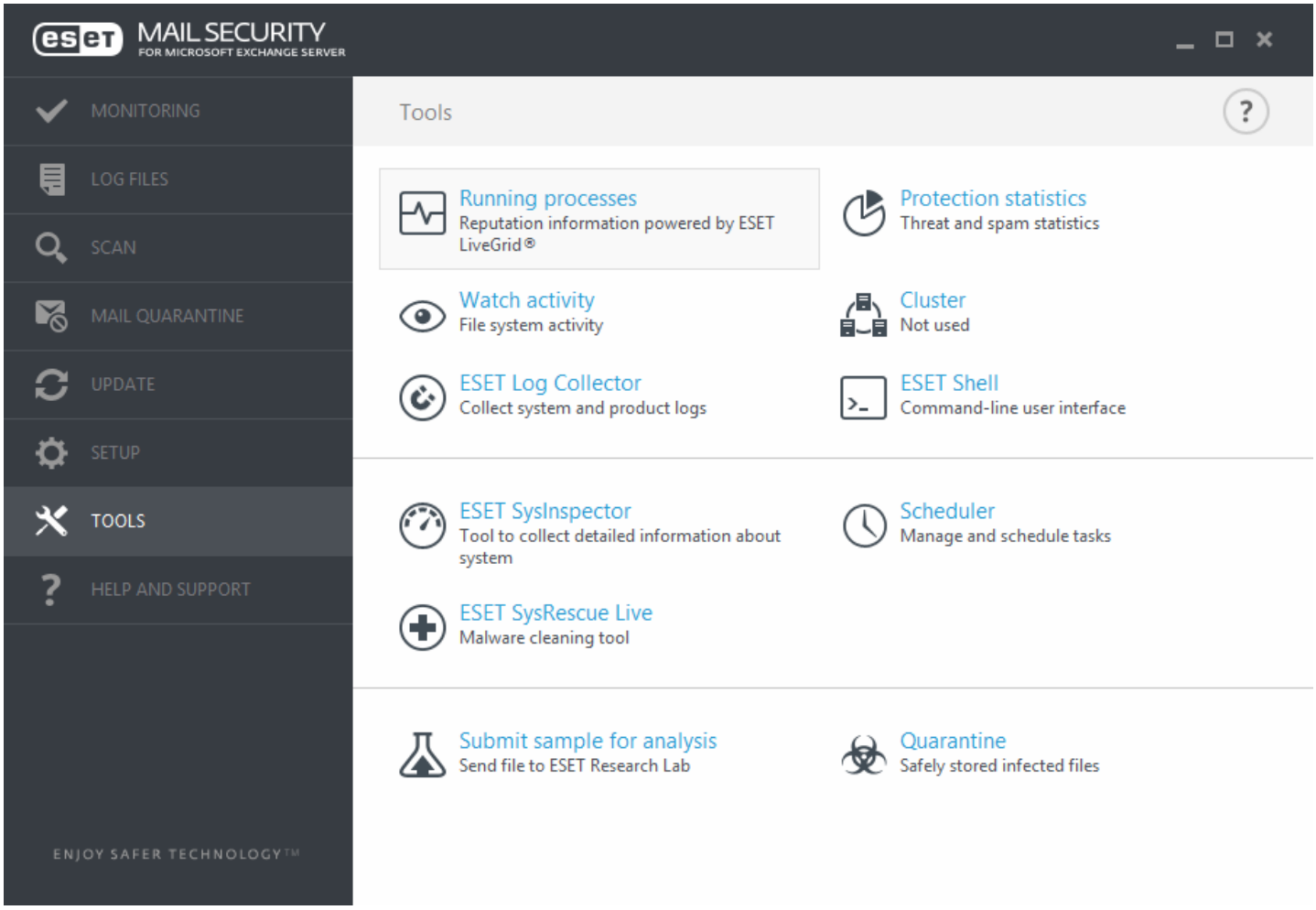
Both import and export use the .xml file type. Import and export are useful if you need to backup the current configuration of ESET Mail Security. It can be used later to apply the same settings to other computer(s).


Import and export settings
The current configuration of ESET Mail Security can be saved to an XML file and restored at a later time when needed.
Import and export
Import settings
Export settings
File name:
...
OK
Cancel

4.7 Tools

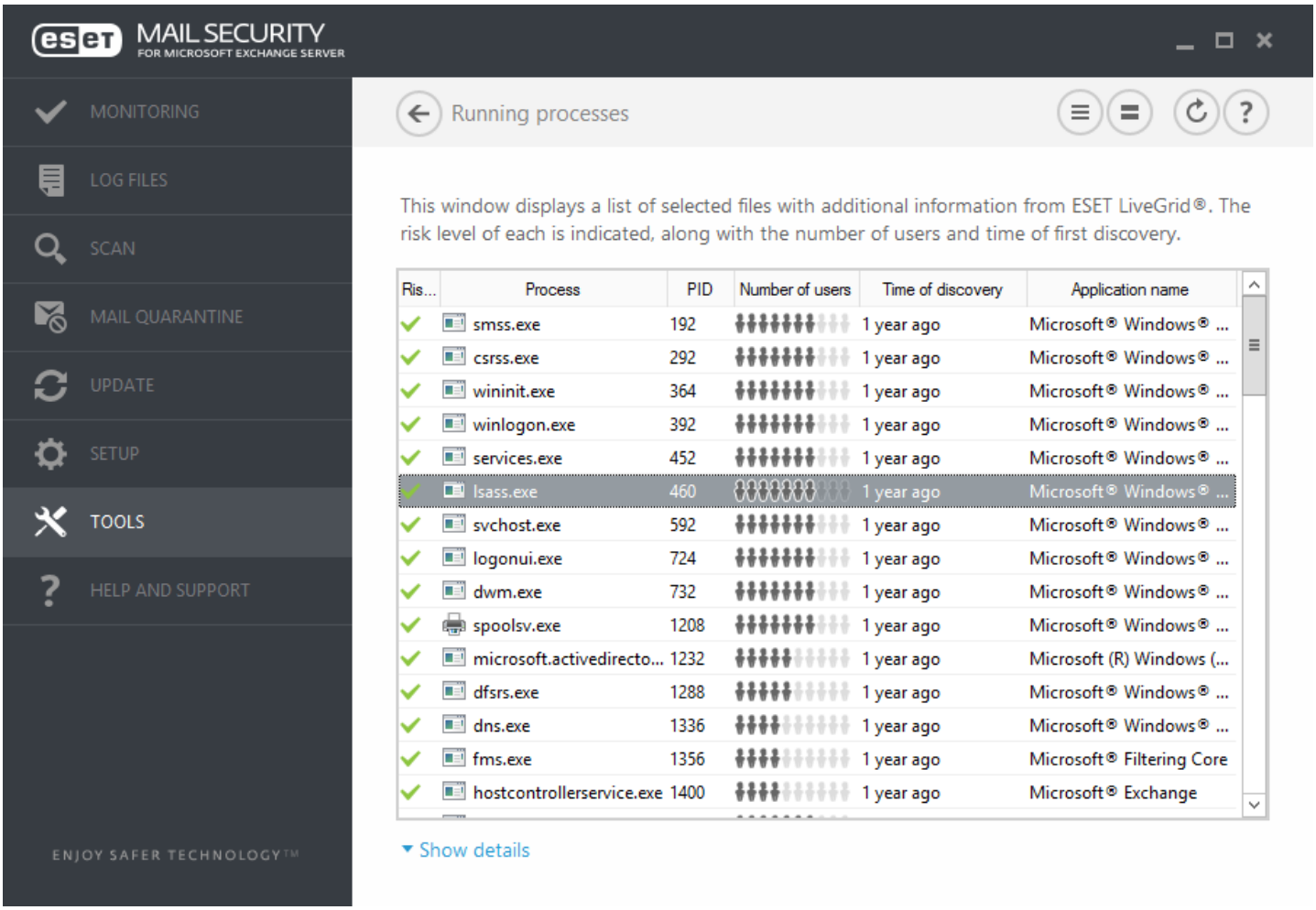
The Tools menu includes modules that help simplify program administration and offer additional options. It includes the following tools:

- Running processes
- Watch activity
- ESET Log Collector
- Protection statistics
- Cluster
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Scheduler
- Submit sample for analysis
- Quarantine



4.7.1 Running processes

Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET Mail Security provides detailed information on running processes to protect users with ESET LiveGrid technology enabled.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
MONITORING
LOG FILES
SCAN
MAIL QUARANTINE
UPDATE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Running processes
This window displays a list of selected files with additional information from ESET LiveGrid®. The risk level of each is indicated, along with the number of users and time of first discovery.
Ris... Process PID Number of users Time of discovery Application name
smss.exe 192 1 year ago Microsoft® Windows® ...
csrss.exe 292 1 year ago Microsoft® Windows® ...
wininit.exe 364 1 year ago Microsoft® Windows® ...
winlogon.exe 392 1 year ago Microsoft® Windows® ...
services.exe 452 1 year ago Microsoft® Windows® ...
lsass.exe 460 1 year ago Microsoft® Windows® ...
svchost.exe 592 1 year ago Microsoft® Windows® ...
logonui.exe 724 1 year ago Microsoft® Windows® ...
dwm.exe 732 1 year ago Microsoft® Windows® ...
spoolsv.exe 1208 1 year ago Microsoft® Windows® ...
microsoft.activedirecto... 1232 1 year ago Microsoft (R) Windows (...
dfsrs.exe 1288 1 year ago Microsoft® Windows® ...
dns.exe 1336 1 year ago Microsoft® Windows® ...
fms.exe 1356 1 year ago Microsoft® Filtering Core
hostcontrollerservice.exe 1400 1 year ago Microsoft® Exchange
Show details

Risk level - In most cases, ESET Mail Security and ESET LiveGrid technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1- Fine (green) to 9- Risky (red).

Process - Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing **Ctrl**+**Shift**+**Esc** on your keyboard.

PID - Is an ID of processes running in Windows operating systems.

NOTE: Known applications marked as Fine (green) are definitely clean (white-listed) and will be excluded from scanning, as this will improve the scanning speed of on-demand computer scan or Real-time file system protection on your computer.

Number of users - The number of users that use a given application. This information is gathered by ESET LiveGrid technology.

Time of discovery - Period of time since the application was discovered by ESET LiveGrid technology.

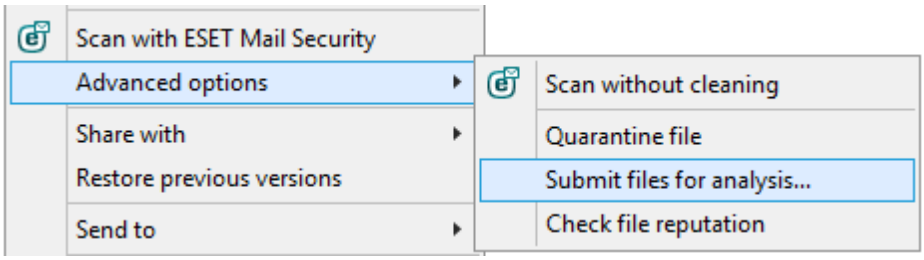
NOTE: When an application is marked as Unknown (orange) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the Submit sample for analysis feature to send the file to the ESET Virus Lab. If the file turns out to be a malicious application, its detection will be added to one of the upcoming Virus Signature Database updates.

Application name - Given name of a program this process belongs to.

By clicking a given application at the bottom, the following information will appear at the bottom of the window:

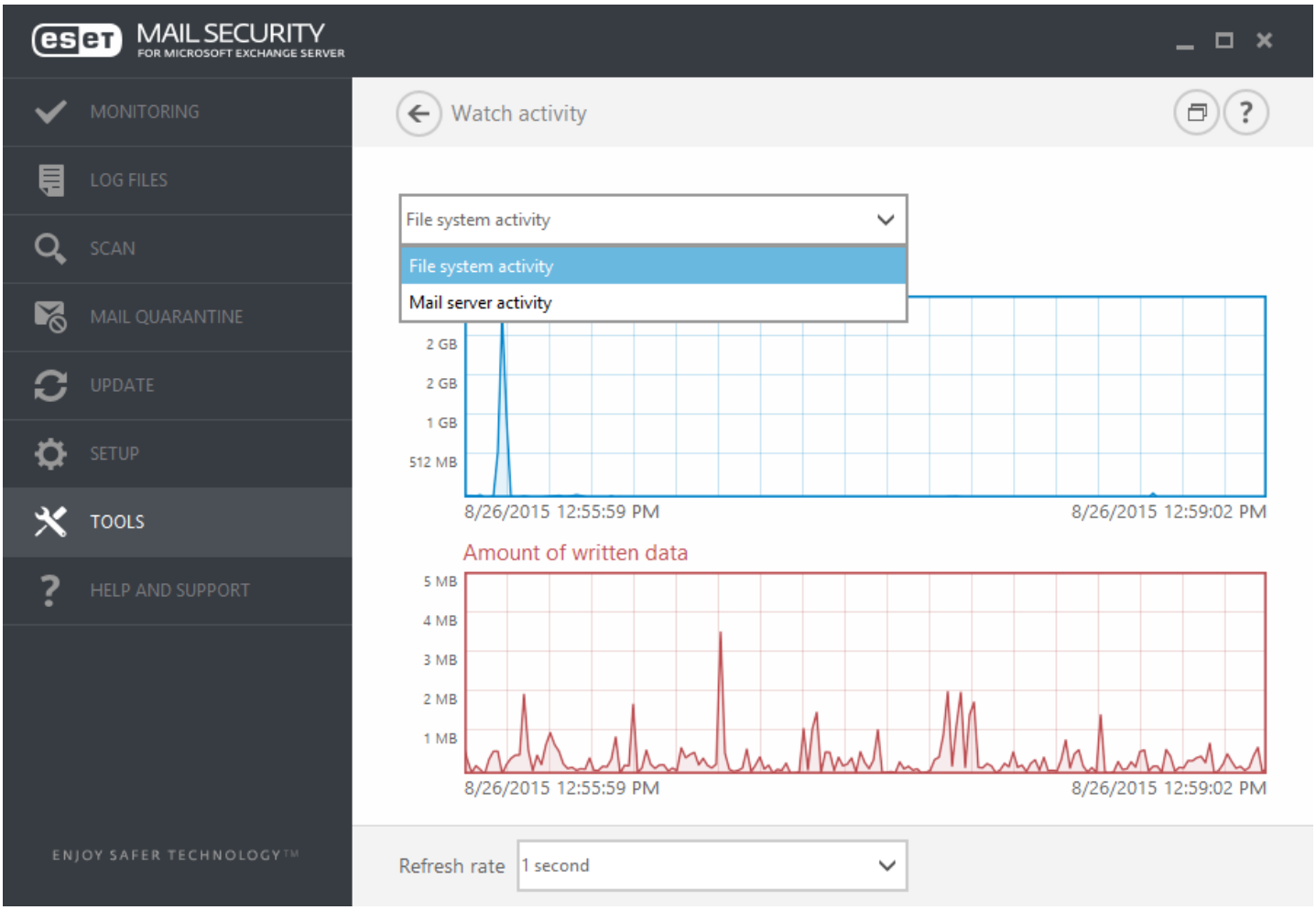
- **Path** - Location of an application on your computer.
- **Size** - File size either in kB (kilobytes) or MB (megabytes).
- **Description** - File characteristics based on the description from the operating system.
- **Company** - Name of the vendor or application process.
- **Version** - Information from the application publisher.
- **Product** - Application name and/or business name.
- **Created on** - Date and time when an application was created.
- **Modified on** - Last date and time when an application was modified.

NOTE: Reputation can also be checked on files that do not act as running programs/processes - mark files you want to check, right-click on them and from the context menu select **Advanced options** > **Check File Reputation using ESET LiveGrid**.



4.7.2 Watch activity

To see the current **File system activity** and **Mail server activity** in graph form, click **Tools** > **Watch activity**. It shows you the amount of read and written data in your system in two graphs. At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. To change the time span, select from **Refresh rate** drop-down menu.



The following options are available:

- **1 second** - The graph refreshes every second and the timeline covers the last 10 minutes.
- **1 minute (last 24 hours)** - The graph is refreshed every minute and the timeline covers the last 24 hours.
- **1 hour (last month)** - The graph is refreshed every hour and the timeline covers the last month.
- **1 hour (selected month)** - The graph is refreshed every hour and the timeline covers the selected month. Click **Change month** button to make another selection.

The vertical axis of the **File system activity** graph represents the amount of read data (blue) and the amount of written data (red). Both values are given in kB (kilobytes)/MB/GB. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

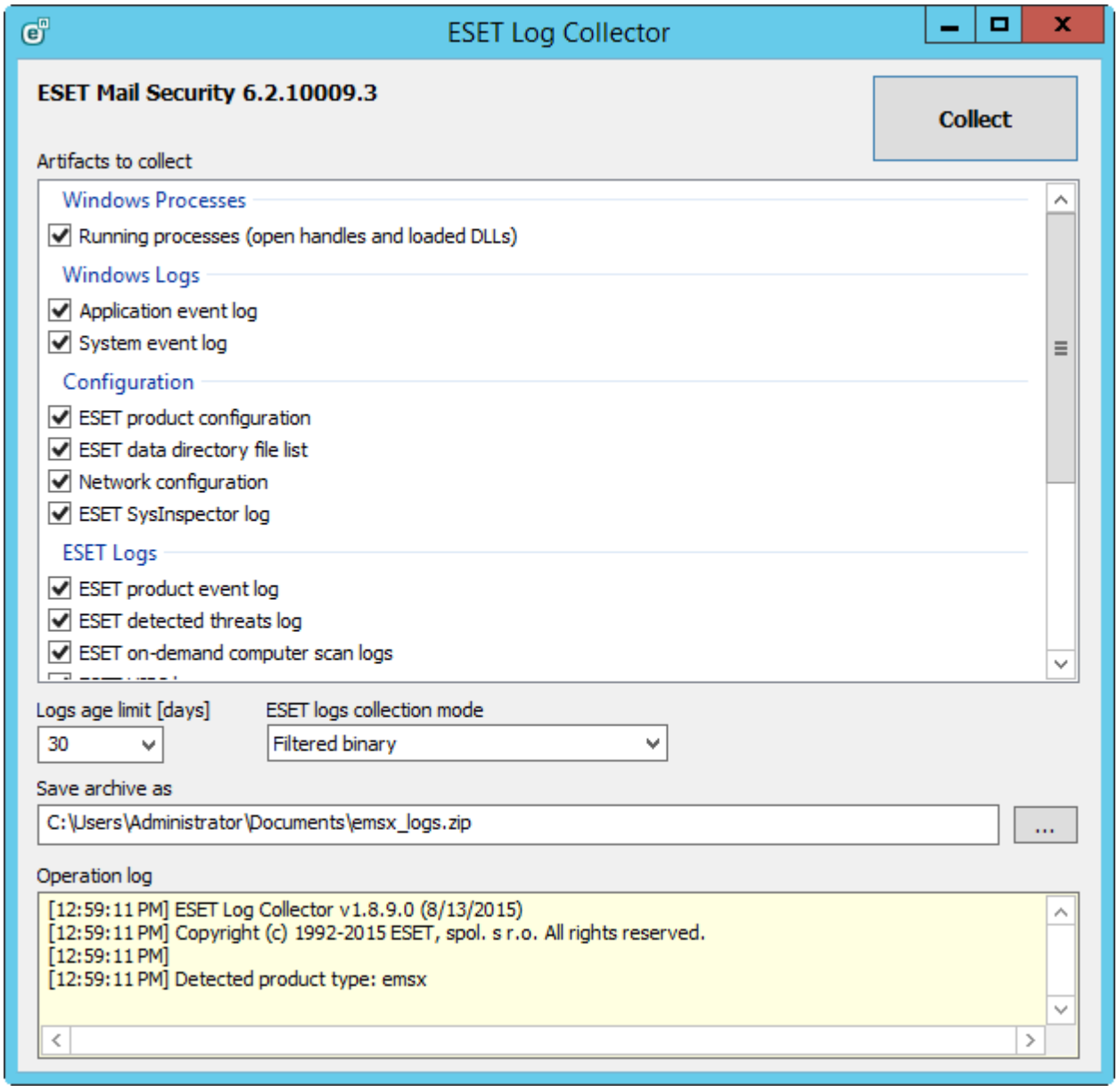
4.7.2.1 Time period selection

Select a month (and a year) for which you want to see **File system activity** or **Mail server activity** in the graph.

4.7.3 ESET Log Collector

ESET Log Collector is an application that automatically collects information, such as configuration and logs from your server in order to help resolve issues more quickly. When you have a case open with ESET Customer Care, you may be asked to provide logs from your computer. ESET Log Collector will make it easy for you to collect the information needed.

ESET Log Collector is accessible from the main menu by clicking **Tools** > **ESET Log Collector**.



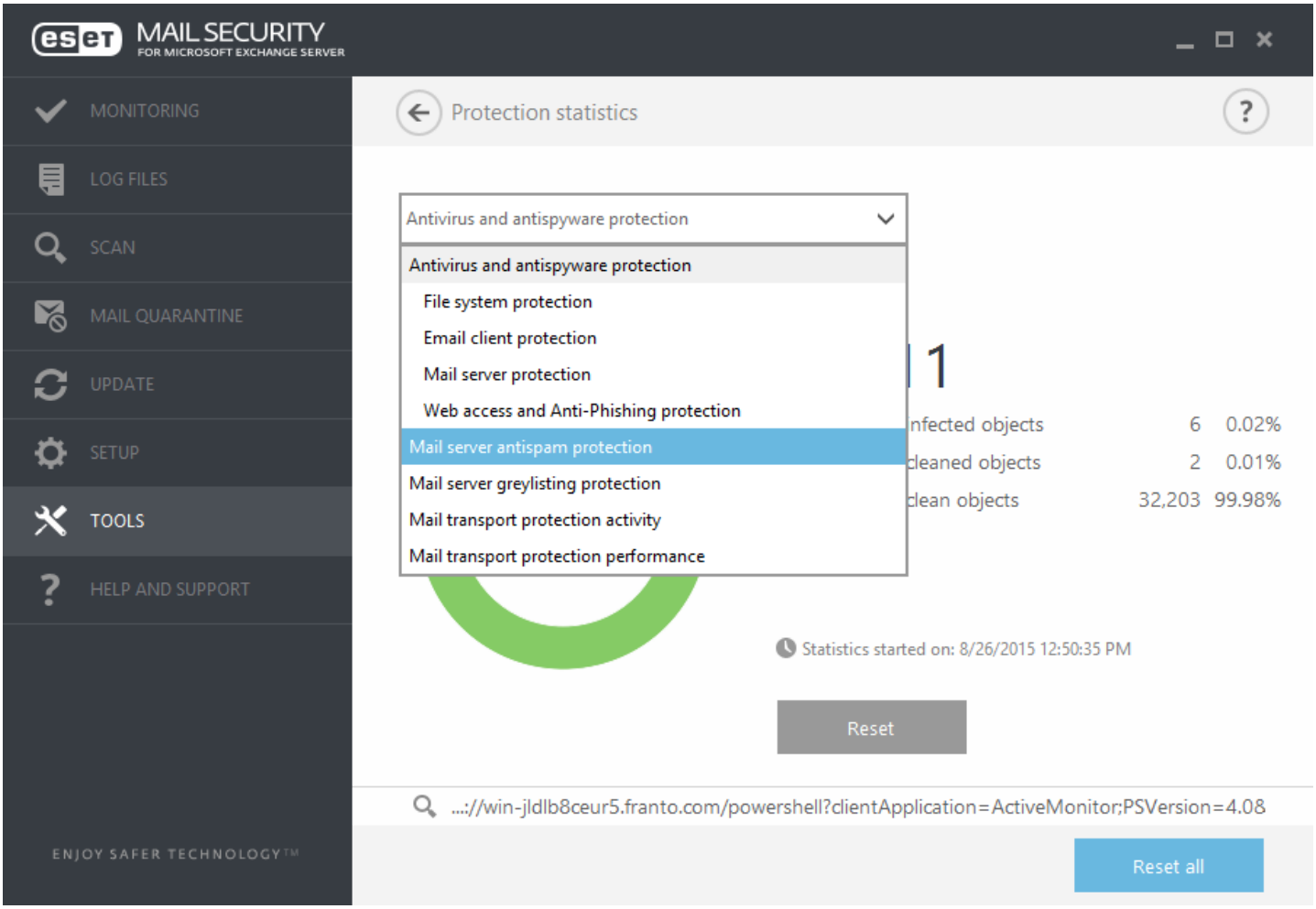
Select the appropriate check boxes for the logs that you want to collect. If you are unsure what to select, leave all check boxes selected (default). Specify the location where you want to save archive files and then click **Save**. The archive file name is already predefined. Click **Collect**.

During the collection, you can view the operation log window at the bottom to see what operation is currently in progress. When collection is finished, all files have been collected and archived will be displayed. This means that collection was successful and the archive file (for example, `emsx_logs.zip`) has been saved in the location specified.

For further information about ESET Log Collector and for the list of files that ESET Log Collector actually collects, please visit the ESET Knowledgebase.

4.7.4 Protection statistics

To view a graph of statistical data related to protection modules in ESET Mail Security, click **Tools** > **Protection statistics**. Select the desired protection module from the drop-down menu to see the corresponding graph and legend. Mouse over an item in the legend to display data for that item in the graph.



The following statistic graphs are available:

- **Antivirus and antispyware protection** - Displays the overall number of infected and cleaned objects.
- **File system protection** - Displays objects that were read or written to the file system only.
- **Email client protection** - Displays objects that were sent or received by email clients only.
- **Mail server protection** - Displays antivirus and antispyware mail server statistics.
- **Web access and Anti-Phishing protection** - Displays objects downloaded by web browsers only.
- **Mail server antispam protection** - Displays the history of antispam statistics since the last start up.
- **Mail server greylisting protection** - Includes antispam statistic generated using the greylisting method.
- **Mail transport protection activity** - Displays objects verified/blocked/deleted by the mail server.
- **Mail transport protection performance** - Displays data processed by VSAPI/Transport Agent in B/s.
- **Mailbox database protection activity** - Displays objects processed by VSAPI (number of **verified**, **quarantined** and **deleted objects**).
- **Mailbox database protection performance** - Displays data processed by VSAPI (number of different averages for **Today**, for **Last 7 days** and averages **Since last reset**).

Next to the statistics graphs, you can see the number of all scanned, infected, cleaned and clean objects. Click **Reset** to clear statistics information, or click **Reset all** to clear and remove all existing data.

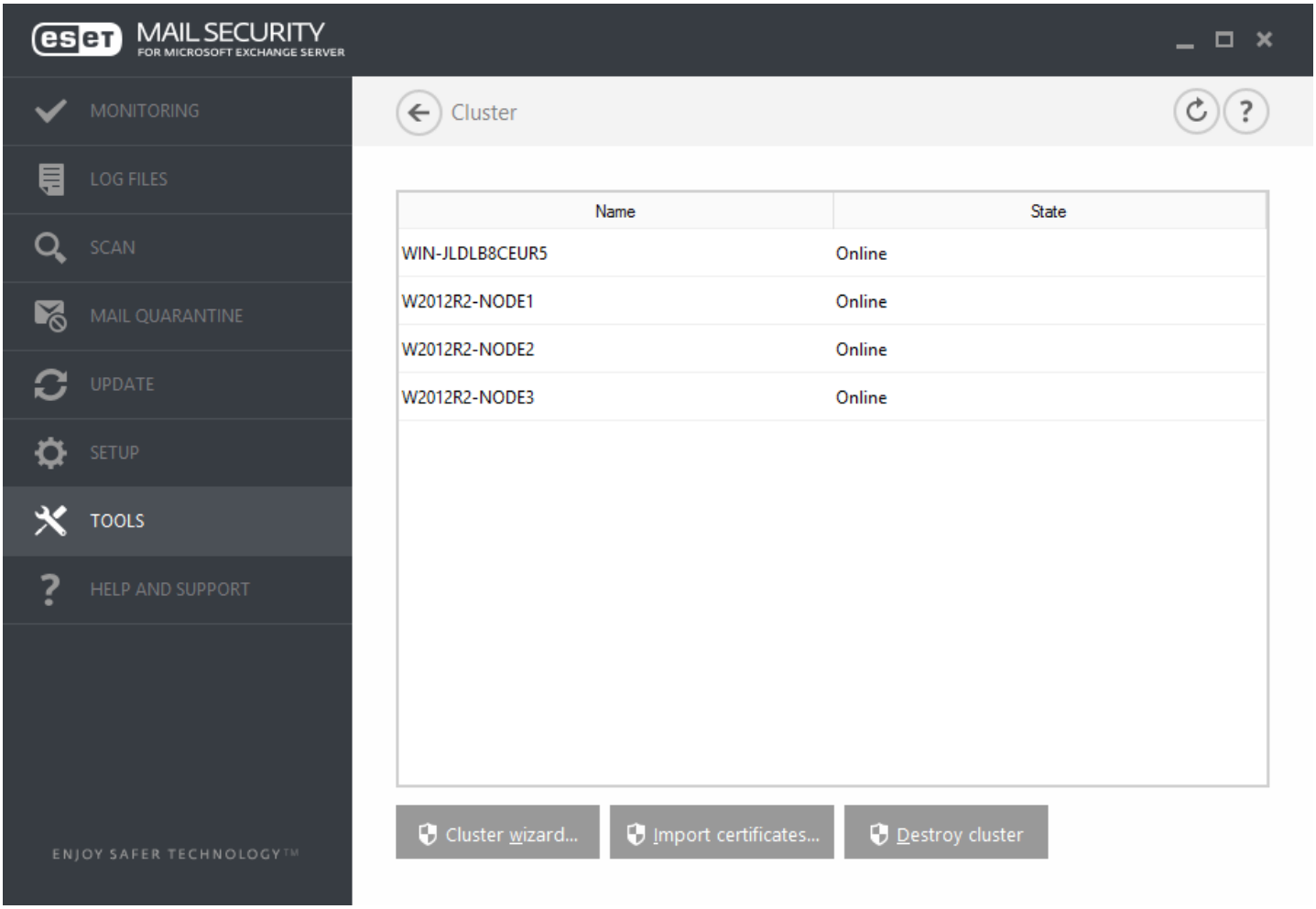
4.7.5 Cluster

The **ESET Cluster** is a P2P communication infrastructure of the ESET line of products for Microsoft Windows Server.

This infrastructure enables ESET server products to communicate with each other and exchange data such as configuration and notifications as well as synchronize data necessary for correct operation of a group of product instances. An example of such group is a group of nodes in a Windows Failover Cluster or Network Load Balancing (NLB) Cluster with ESET product installed where there is a need to have the same configuration of the product across the whole cluster. ESET Cluster ensures this consistency between instances.

NOTE: User interface settings are not being synchronized between ESET Cluster nodes.

The ESET Cluster status page is accessible from the main menu in **Tools** > **Cluster** when properly configured, the status page should look like this:



To setup the ESET Cluster click **Cluster wizard...** For details on how to set the ESET Cluster up using the wizard click here.

When setting up the ESET Cluster, there two ways to add nodes - automatically using existing Windows Failover Cluster / NLB Cluster or manually by browsing for computers that are in a Workgroup or in a Domain.

Autodetect - Automatically detects nodes that are already members of a Windows Failover Cluster / NLB Cluster and adds the to the ESET Cluster
Browse - You can add nodes manually by typing in the server names (either members of the same Workgroup or members of the same Domain)

NOTE: Servers don't have to be members of a Windows Failover Cluster / NLB Cluster to use the ESET Cluster feature. A Windows Failover Cluster or NLB Cluster in your is not required in your environment for you to use ESET clusters.

Once you have added nodes to your ESET Cluster, the next step is the installation of ESET Mail Security on each node. This is done automatically during ESET Cluster setup.

Credentials that are required for remote installation of ESET Mail Security on other cluster nodes:

- Domain scenario - domain administrator credentials
- Workgroup scenario - you need to make sure that all nodes use the same local administrator account credentials

In an ESET Cluster, you can also use a combination of nodes added automatically as members of an existing Windows Failover Cluster / NLB Cluster and nodes added manually (provided they are in the same Domain).

NOTE: It is not possible to combine Domain nodes with Workgroup nodes.

Another requirement for the use of an ESET Cluster is that **File and Printer Sharing** must be enabled in Windows Firewall before pushing ESET Mail Security installation to the ESET Cluster nodes.

ESET Cluster can easily be dismantled by clicking **Destroy cluster**. Each node will write a record in their event log about the ESET Cluster being destroyed. After that, all ESET firewall rules are removed from the Windows Firewall. Former nodes will be reverted to their previous state and can be used again in other ESET Cluster if necessary.

NOTE: The creation of ESET Clusters between ESET Mail Security and ESET File Security for Linux is not supported.

Adding new nodes to an existing ESET Cluster can be done anytime by running the **Cluster wizard** as described above and here.

4.7.5.1 Cluster wizard - page 1

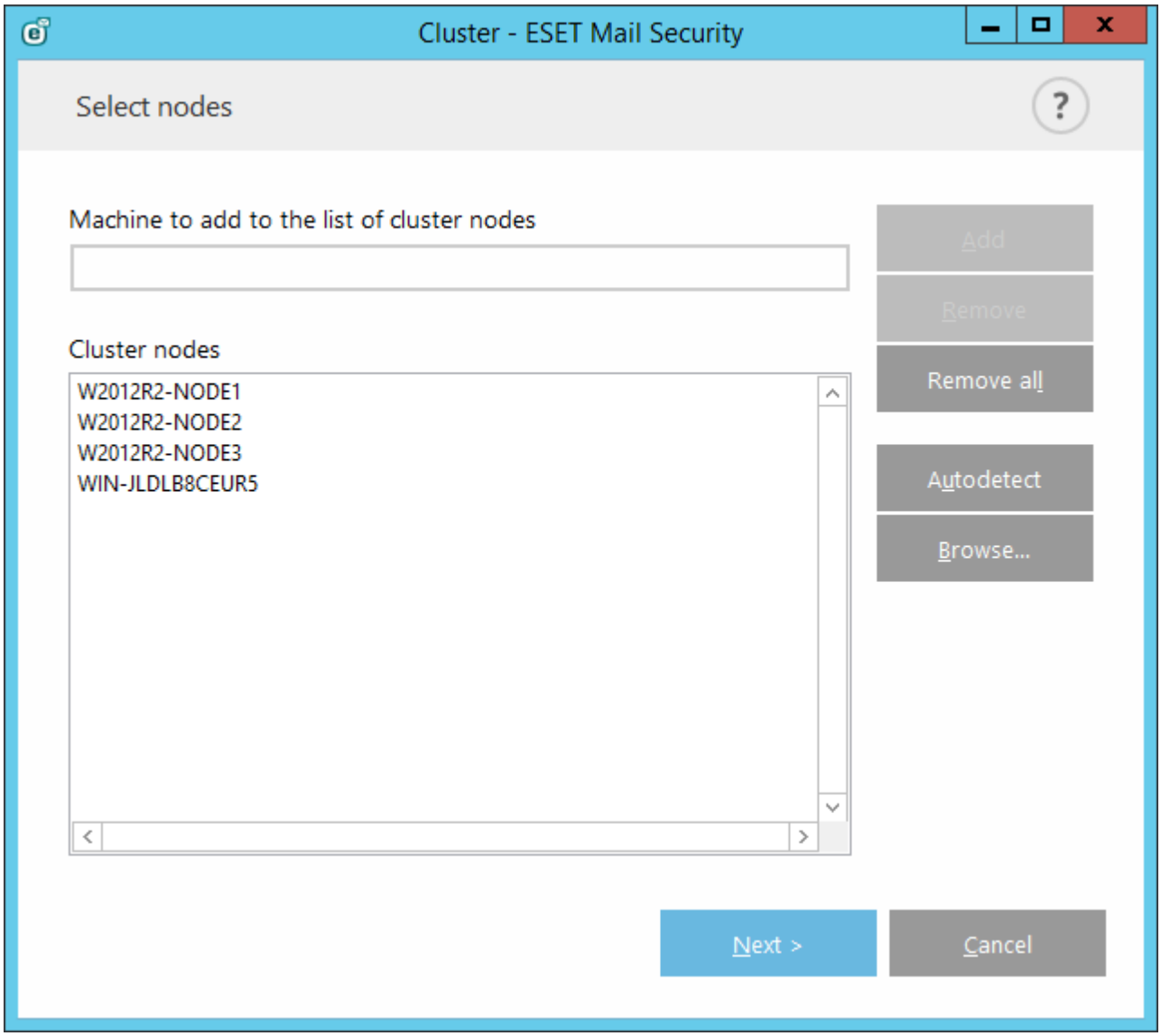
The first step when setting up an ESET Cluster is adding nodes. You can either use the **Autodetect** option or **Browse** to add nodes. Alternatively, you can type the server name into the text box and click **Add**.

Autodetect automatically adds nodes from an existing Windows Failover Cluster / Network Load Balancing (NLB) Cluster. The server you are using to create the ESET Cluster from needs to be a member of this Windows Failover Cluster / NLB Cluster in order to automatically add the nodes. The NLB Cluster must have the **Allow remote control** feature enabled in cluster properties for ESET Cluster to detect the nodes correctly. Once you have the list of newly added nodes, you can remove unwanted ones, in case you only want specific nodes in the ESET Cluster.

Click **Browse** to find and select computers within a Domain or a Workgroup. This method allows for manual addition of nodes to the ESET Cluster.

Another way to add nodes is by typing the host name of the server you want add and clicking **Add**.

Current **Cluster nodes** chosen to be added to the ESET Cluster after clicking **Next**:



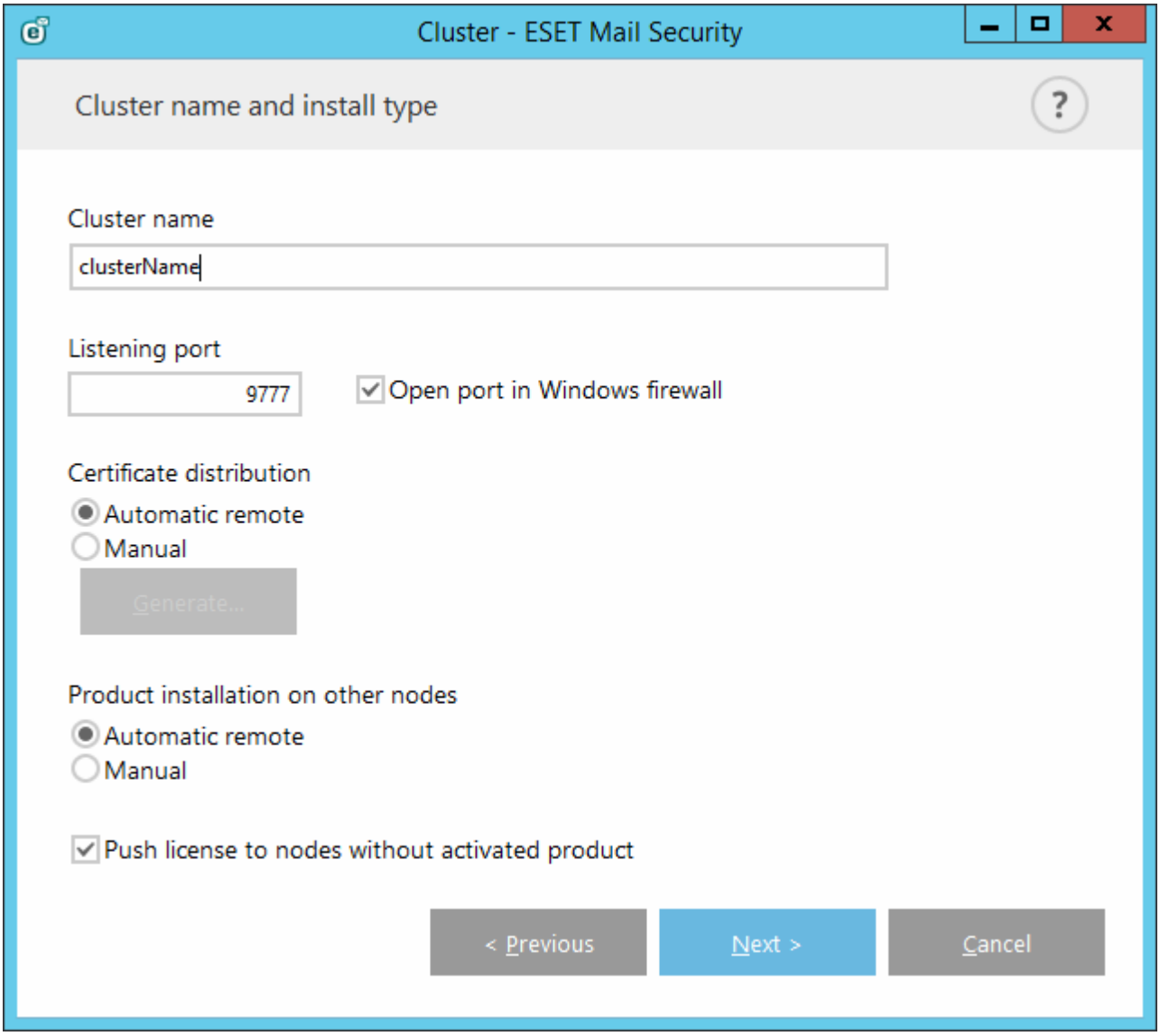
To modify **Cluster nodes** in the list, select the node you want to remove and click **Remove**, or to clear the list completely click **Remove all**.

If you already have an existing ESET Cluster, you can add new nodes into it at any time. The steps are the same as described above.

NOTE: All nodes that remain in the list must be online and reachable. Localhost is added into the cluster nodes by default.

4.7.5.2 Cluster wizard - page 2

Define a cluster name, certificate distribution mode and whether to install the product on the other nodes or not.



Cluster name - type your cluster name.
Listening port - (default port is 9777)
Open port in Windows firewall - when checked a rule is created in the Windows Firewall.

Certificate distribution:
Automatic remote - certificate will be installed automatically.
Manual - when you click **Generate** a browse window will open - select the folder in which to store certificates. A root certificate as well as a certificate for each node, including the one (local machine) from which you are setting up the ESET Cluster, will be created. You can then choose to enroll the certificate to local machine by clicking **Yes**. You will later need to import certificates manually as described here.

Product install to other nodes:
Automatic remote - ESET Mail Security will be installed automatically on each node (provided their operating systems are the same architecture).
Manual - Choose this if you want to install ESET Mail Security manually (for example when you have different OS architectures on some of the nodes).

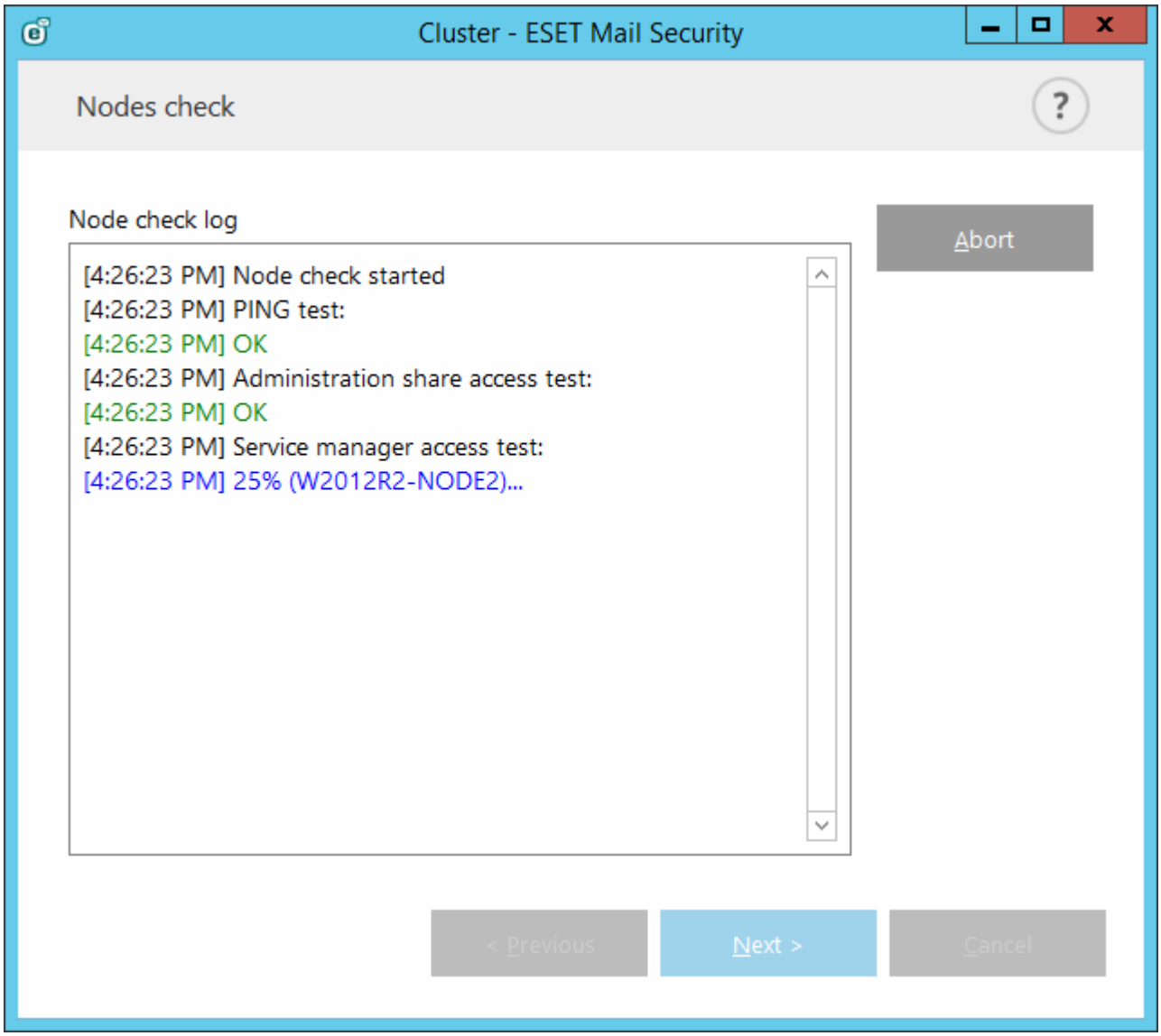
Push license to nodes without activated product - when checked, nodes will get ESET Mail Security activated.

NOTE: If you want to create ESET Cluster with mixed operating system architectures (32 bit and 64 bit), then you will need to install ESET Mail Security manually. This will be detected during next steps and you'll see this information in the log window.

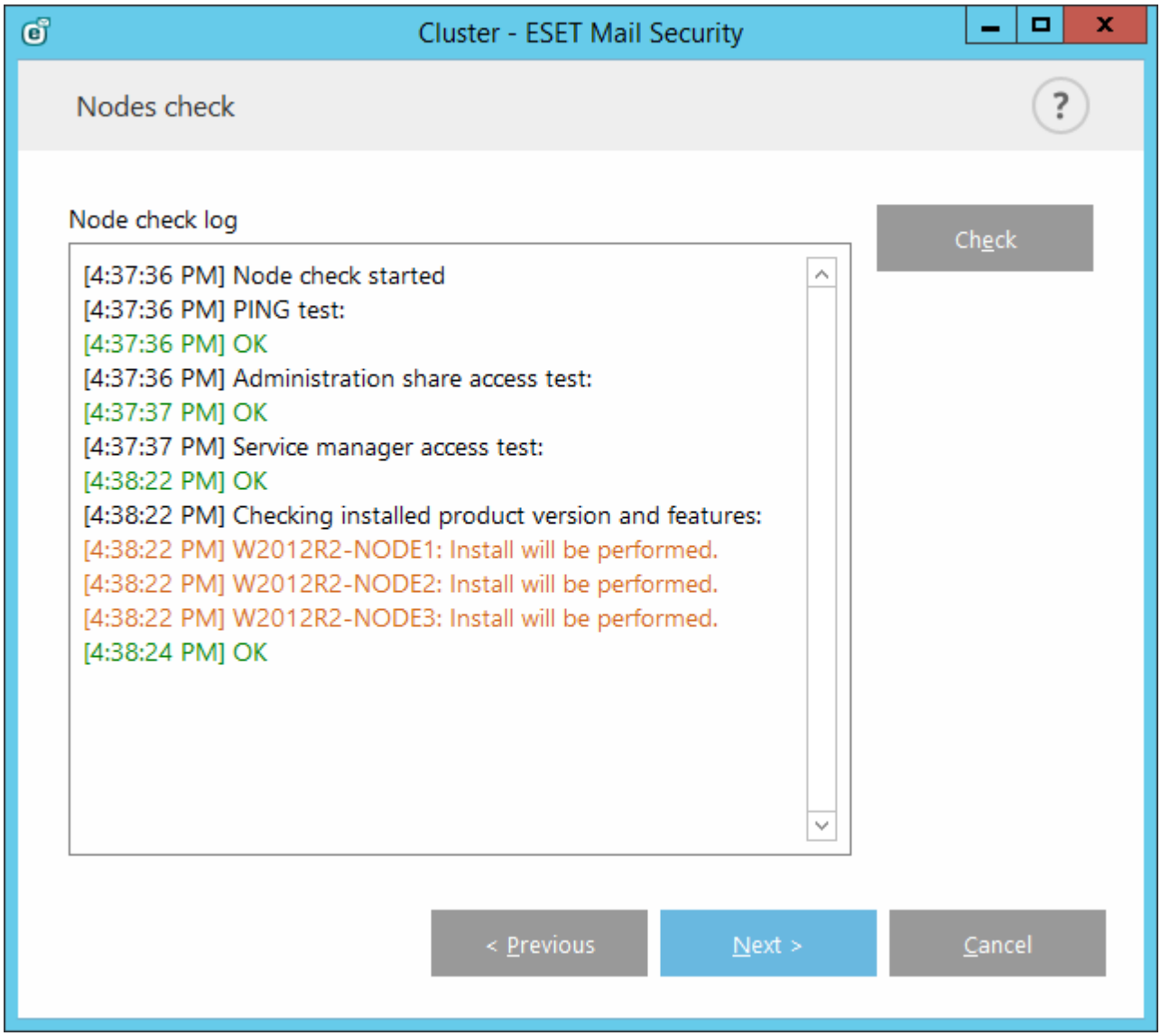
4.7.5.3 Cluster wizard - page 3

After specifying installation details a node check is run. You will see following being checked in the **Nodes check log**:

- check that all existing nodes are online
- check that new nodes are accessible
- node is online
- admin share is accessible
- remote execution is possible
- correct version of product is installed, or no product (only if auto install selected)
- check that the new certificates are present

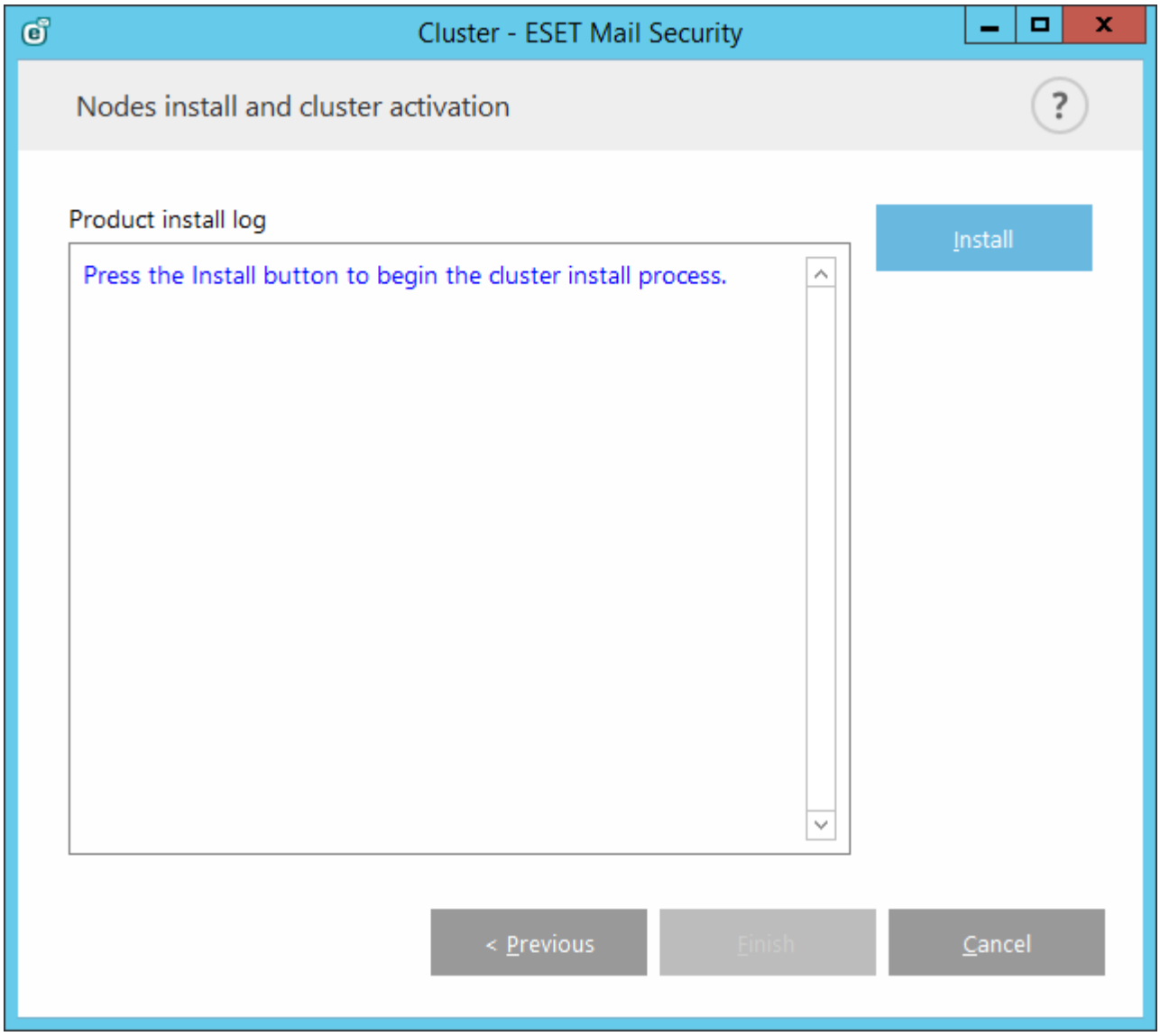


You will see the report once the node check is finished:


Cluster - ESET Mail Security
Nodes check
Node check log
Check
[4:37:36 PM] Node check started
[4:37:36 PM] PING test:
[4:37:36 PM] OK
[4:37:36 PM] Administration share access test:
[4:37:37 PM] OK
[4:37:37 PM] Service manager access test:
[4:38:22 PM] OK
[4:38:22 PM] Checking installed product version and features:
[4:38:22 PM] W2012R2-NODE1: Install will be performed.
[4:38:22 PM] W2012R2-NODE2: Install will be performed.
[4:38:22 PM] W2012R2-NODE3: Install will be performed.
[4:38:24 PM] OK
< Previous
Next >
Cancel

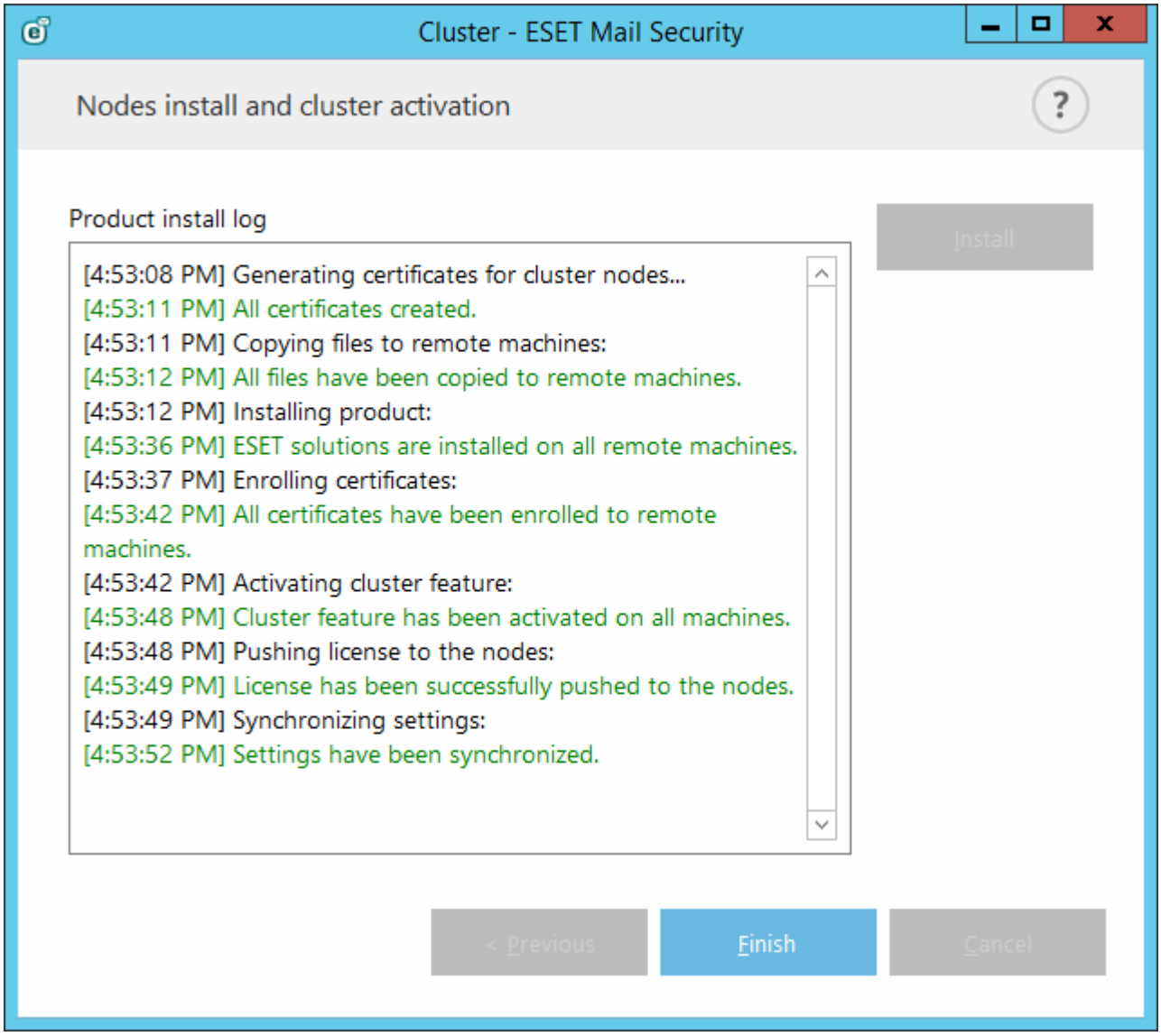
4.7.5.4 Cluster wizard - page 4

When the product has to be installed on a remote machine during ESET Cluster initialization, the installer package checks %ProgramData%\ESET\<Produt_name>\Installer directory for presence of the installer. If the installer package is not found there, the user is asked to locate one.

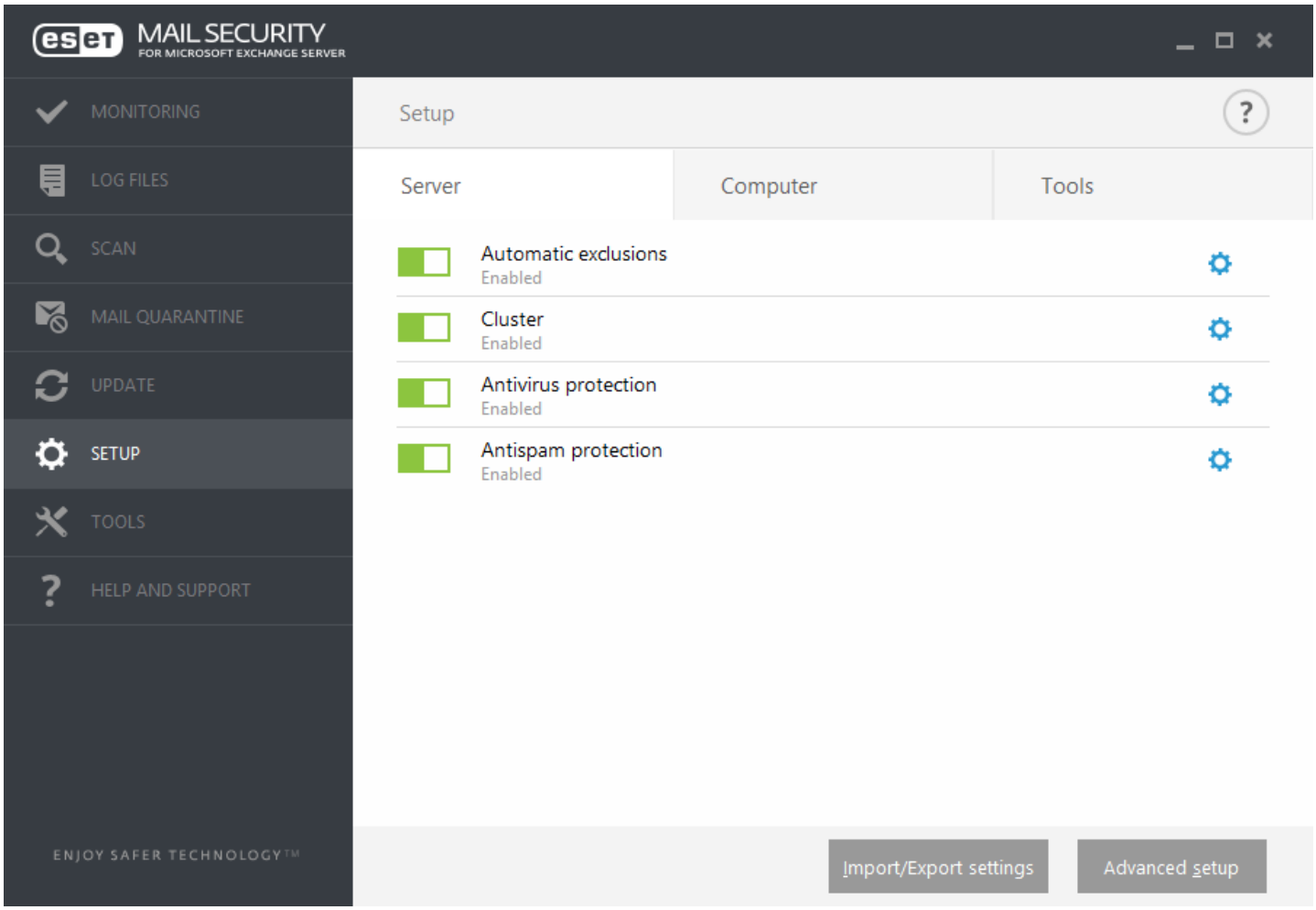


NOTE: When trying to use automatic remote installation for a node with different platform (32-bit vs 64-bit), this will be detected and manual installation will be recommended for such node.

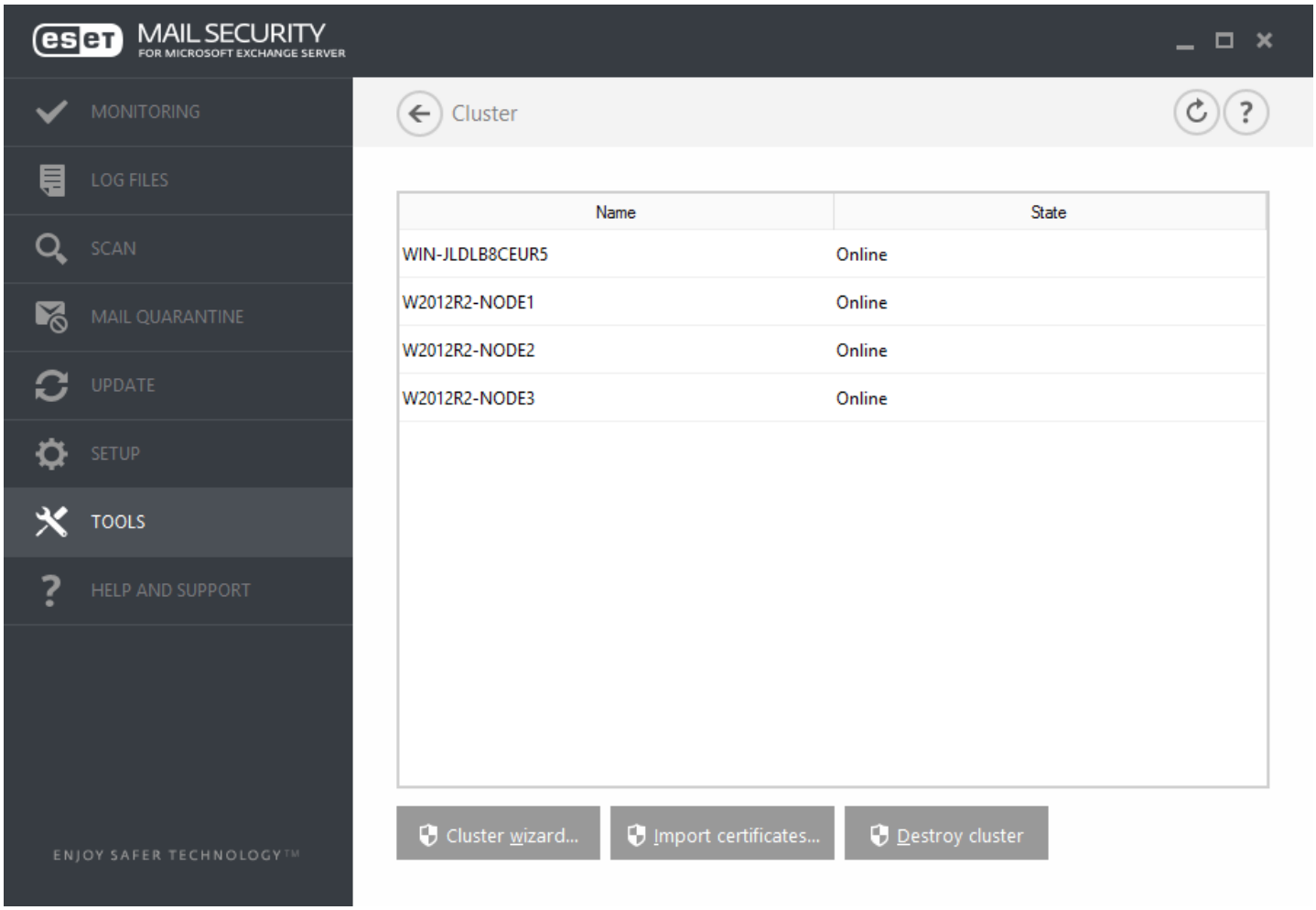
NOTE: If you have an older version of ESET Mail Security already installed on some nodes, then ESET Mail Security needs to be reinstalled with a newer version on these machines before creating the cluster. This may cause an automatic restart of those machines. You'll see a warning should this be the case.


Cluster - ESET Mail Security
Nodes install and cluster activation
Product install log
Install
[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.
< Previous
Finish
Cancel

Once you have correctly configured the ESET Cluster, it will appear in **Setup** > **Server** page as enabled.



Also, you can check its current status in Cluster status page (**Tools** > **Cluster**).



Import certificates...

- Navigate to the folder that contains the certificates (generated during the use of Cluster wizard). Select the certificate file and click **Open**.

4.7.6 ESET Shell

eShell (short for ESET Shell) is a command line interface for ESET Mail Security. It is an alternative to the graphical user interface (GUI). eShell has all the features and options that the GUI normally gives you. eShell lets you configure and administer the whole program without the use of the GUI.

Apart from all the functions and features that are available in the GUI, it also provides you with the option of using automation by running scripts in order to configure, modify configuration or perform an action. Also, eShell can be useful for those who prefer using the command line over the GUI.

There are two modes in which eShell can be run:

- Interactive mode - this is useful when you want to work with eShell (not just execute single command) for tasks such as changing configuration, viewing logs, etc. You can also use interactive mode if you are not familiar with the all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.
- Single command / Batch mode - you can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in `eshell` with appropriate parameters. For example:

```
eshell get status
```

or

```
eshell set antivirus status disabled
```

In order to run certain commands (such as second example above) in batch/script mode, there are a couple of settings that you need to configure first. Otherwise, you'll get **Access Denied** message. This is for security reasons.

NOTE: For full functionality we recommend you to open the eShell using **Run as administrator**. The same applies when executing single command via Windows Command Prompt (cmd). Open the cmd using **Run as administrator**. Otherwise you won't be able to execute all commands. It is because when you open cmd or eShell using other account than administrator you will not have sufficient permissions.

NOTE: In order to run eShell commands from Windows Command Prompt or to run batch files, you need to make some settings. For further information about running batch files click here.

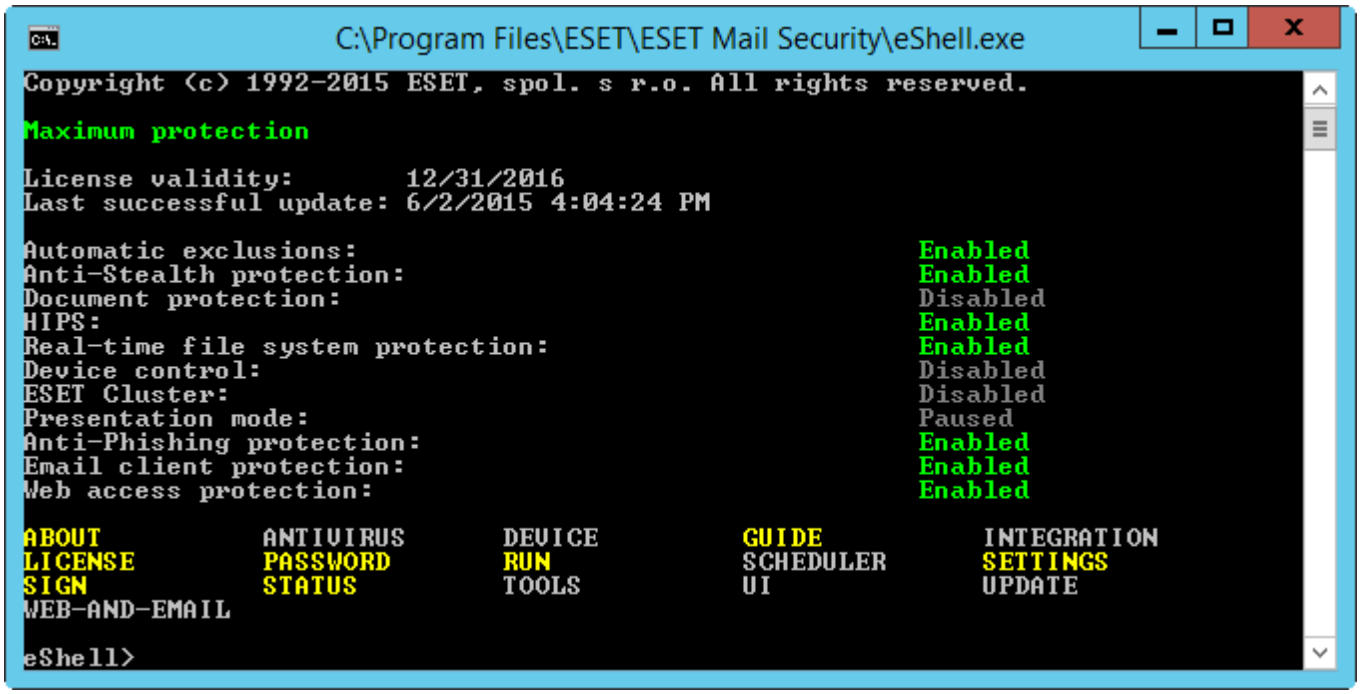
To enter interactive mode in eShell, you can use one of the following two methods:

- Via Windows Start menu: **Start** > **All Programs** > **ESET** > **ESET Mail Security** > **ESET shell**
- From Windows Command Prompt by typing in `eshell` and pressing the Enter key

When you run eShell in interactive mode for the first time, a first run (guide) screen will display.

NOTE: If you want to display the first run screen in future, type in `guide` command. It shows you some basic examples how to use eShell with Syntax, Prefix, Command path, Abbreviated forms, Aliases, etc. This is basically a quick guide to eShell.

Next time you run eShell, you'll see this screen:



NOTE: Commands are not case sensitive. You can use upper case (capital) or lower case letters and the command will execute regardless.

Customizing eShell

You can customize eShell in `ui eshell` context. You can configure aliases, colors, language, execution policy for scripts, you can choose to display hidden commands, and some others settings.

4.7.6.1 Usage

Syntax
Commands must be formatted in the correct syntax to function and can be composed of a prefix, context, arguments, options, etc. This is the general syntax used throughout the eShell:

[<prefix>] [<command path>] <command> [<arguments>]

Example (this activates document protection):
`SET ANTIVIRUS DOCUMENT STATUS ENABLED`

`SET` - a prefix
`ANTIVIRUS DOCUMENT` - path to a particular command, a context where this command belong
`STATUS` - the command itself
`ENABLED` - an argument for the command

Using `?` as an argument for command will display the syntax for that particular command. For example, `STATUS ?` will show you the syntax for `STATUS` command:

SYNTAX:

```
[get] | status
set status enabled | disabled
```

You may notice that `[get]` is in brackets. It designates that the prefix `get` is default for the `status` command. This means that when you execute `status` without specifying any prefix, it will actually use the default prefix (in this case `get status`). Using commands without a prefix saves time when typing. Usually `get` is the default prefix for most commands, but you need to be sure what the default prefix is for a particular command and that it is exactly what you want to execute.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Prefix / Operation
A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET Mail Security is configured or show you the status (such as `GET ANTIVIRUS STATUS` will show you current protection status). The `SET` prefix will configure functionality or change its status (`SET ANTIVIRUS STATUS ENABLED` will activate protection).

These are the prefixes that eShell lets you use. A command may or may not support any of the prefixes:

- `GET` - returns current setting/status
- `SET` - sets value/status
- `SELECT` - selects an item
- `ADD` - adds an item
- `REMOVE` - removes an item
- `CLEAR` - removes all items/files
- `START` - starts an action
- `STOP` - stops an action
- `PAUSE` - pauses an action
- `RESUME` - resumes an action
- `RESTORE` - restores default settings/object/file
- `SEND` - sends an object/file
- `IMPORT` - imports from a file
- `EXPORT` - exports to a file

Prefixes such as `GET` and `SET` are used with many commands, but some commands (such as `EXIT`) do not use a prefix.

Command path / Context
Commands are placed in contexts which form a tree structure. The top level of the tree is root. When you run eShell, you are at the root level:

```
eShell>
```

You can either execute a command from here, or enter the context name to navigate within the tree. For example, when you enter `TOOLS` context, it will list all commands and sub-contexts that are available from here.

Yellow items are commands you can execute and grey items are sub-contexts you can enter. A sub-context contain further commands.

If you need to return back to a higher level, use `..` (two dots). For example, say you are here:

```
eShell antivirus startup>
```

type `..` and it will get you up one level, to:

```
eShell antivirus>
```

If you want to get back to root from `eShell antivirus startup>` (which is two levels lower from root), simply type `.. ..` (two dots and two dots separated by space). By doing so, you will get two levels up, which is root in this case. Use backslash `\` to return directly to root from any level no matter how deep within the context tree you are. If you want to get to a particular context in upper levels, simply use the appropriate number of `..` as you need to get to the desired level, but use space as a separator. For example, if you want to get three levels higher, use `.. .. ..`

The path is relative to the current context. If the command is contained in the current context, do not enter a path. For example, to execute `GET ANTIVIRUS STATUS` enter:

- `GET ANTIVIRUS STATUS` - if you are in the root context (command line shows `eShell>`)
- `GET STATUS` - if you are in the context `ANTIVIRUS` (command line shows `eShell antivirus>`)
- `.. GET STATUS` - if you are in the context `ANTIVIRUS STARTUP` (command line shows `eShell antivirus startup>`)

NOTE: You can use single `.` (dot) instead of two `..` because single dot is an abbreviation of two dots. For example:

- `. GET STATUS` - if you are in the context `ANTIVIRUS STARTUP` (command line shows `eShell antivirus startup>`)

Argument
An argument an action which is performed for a particular command. For example, command `CLEAN-LEVEL` (located in `ANTIVIRUS REALTIME ENGINE`) can be used with following arguments:

- `no` - No cleaning
- `normal` - Normal cleaning
- `strict` - Strict cleaning

Another example are the arguments `ENABLED` or `DISABLED`, which are used to enable or disable a certain feature or functionality.

Abbreviated form / Shortened commands
eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path.

Examples of the short form:

```
set status enabled    =>    set stat en
add antivirus common scanner-excludes C:\path\file.ext    =>    add ant com scann C:\path\file.ext
```

In a case where two commands or contexts start with same letters (such as ABOUT and ANTIVIRUS, and you enter A as shortened command), eShell will not be able to decide which command of these two you want to run. An error message will display and list commands starting with "A" which you can choose from:

```
eShell>a
The following command is not unique: a

The following commands are available in this context:
   ABOUT - Shows information about program
   ANTIVIRUS - Changes to context antivirus
```

By adding one or more letters (e.g. AB instead of just A) eShell will execute ABOUT command since it is unique now.

NOTE: When you want to be sure that a command executes the way you need, we recommend that you do not abbreviate commands, arguments, etc. and use the full form. This way it will execute exactly as you need and prevent unwanted mistakes. This is especially true for batch files / scripts.

Automatic completion
Is a new feature in eShell since version 2.0. It is very similar to automatic completion in Windows Command Prompt. While Windows Command Prompt completes file paths, eShell completes command, context and operation names as well. Argument completion is not supported. When typing command simply press TAB key to complete or cycle through available variations. Press SHIFT + TAB to cycle backwards. Mixing abbreviated form and automatic completion is not supported. Use either one or the other. For example, when you type `antivir real scan` hitting TAB key will do nothing. Instead, type `antivir` and then TAB to complete `antivirus`, continue typing real + TAB and scan + TAB. You can then cycle through all available variations: scan-create, scan-execute, scan-open, etc.

Aliases
An alias is an alternative name which can be used to execute a command (provided that the command has an alias assigned). There are a few default aliases:

`(global) close` - exit
`(global) quit` - exit
`(global) bye` - exit
`warnlog` - tools log events
`virlog` - tools log detections
`antivirus on-demand log` - tools log scans

"(global)" means that the command can be used anywhere regardless of current context. One command can have multiple aliases assigned, for example command EXIT has alias CLOSE, QUIT and BYE. When you want to exit eShell, you can use the EXIT command itself or any of its aliases. Alias VIRLOG is an alias for command DETECTIONS which is located in TOOLS LOG context. This way the detections command is available from ROOT context, making it easier to access (you don't have to enter TOOLS and then LOG context and run it directly from ROOT).

eShell allows you to define your own aliases. Command ALIAS can be found in UI ESHELL context.

Password protected settings
ESET Mail Security settings can be protected by a password. You can set password using GUI or eShell using `set ui access lock-password` command. You'll then have to enter this password interactively for certain commands (such as those that change settings or modify data). If you plan to work with eShell for a longer period of time and do not want to enter the password repeatedly, you can get eShell to remember the password using `set password` command. Your password will then be filled-in automatically for each executed command that require password. It is remembered until you exit eShell, this means that you'll need to use `set password` again when you start new

session and want eShell to remember your password.

Guide / Help
When you run the `GUIDE` or `HELP` command, it will display a "first run" screen explaining how to use eShell. This command is available from the `ROOT` context (`eShell>`).

Command history
eShell keeps history of previously executed commands. This applies only to the current eShell interactive session. Once you exit eShell, the command history will be dropped. Use the Up and Down arrow keys on your keyboard to navigate through the history. Once you find the command you were looking for, you can execute it again, or modify it without having to type in the entire command from the beginning.

CLS / Clear screen
The `CLS` command can be used to clear screen. It works the same way as it does with Windows Command Prompt or similar command line interfaces.

EXIT / CLOSE / QUIT / BYE
To close or exit eShell, you can use any of these commands (`EXIT`, `CLOSE`, `QUIT` or `BYE`).

4.7.6.2 Commands

This section lists a few basic eShell commands with description as an example.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Example commands (contained within ROOT context):

ABOUT

Lists information about the program. It shows name of the product installed, version number, installed components (including version number of each component) and basic information about the server and the operating system that ESET Mail Security is running on.

CONTEXT PATH:

```
root
```

PASSWORD

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable antivirus protection and those that may affect ESET Mail Security functionality. You will be prompted for password every time you execute such command. You can define this password in order to avoid entering password every time. It will be remembered by eShell and automatically be used when a password-protected command is executed. This means that you do not have to enter the password every time.

NOTE: Defined password works only for the current eShell interactive session. Once you exit eShell, this defined password will be dropped. When you start eShell again, the password needs to be defined again.

This defined password is also very useful when running batch files / scripts. Here is an example of a such batch file:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

This concatenated command above starts a batch mode, defines password which will be used and disables protection.

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERATIONS:

`get` - Show password

`set` - Set or clear password

`restore` - Clear password

ARGUMENTS:

`plain` - Switch to enter password as parameter

`password` - Password

EXAMPLES:

`set password plain <yourpassword>` - Sets a password which will be used for password-protected commands

`restore password` - Clears password

EXAMPLES:

`get password` - Use this to see whether the password is configured or not (this is only shows only stars "*", does not list the password itself), when no stars are visible, it means that there is no password set

`set password plain <yourpassword>` - Use this to set defined password

`restore password` - This command clears defined password

STATUS

Shows information about the current protection status of ESET Mail Security (similar to GUI).

CONTEXT PATH:

`root`

SYNTAX:

`[get] | restore status`

`set status disabled | enabled`

OPERATIONS:

`get` - Show antivirus protection status

`set` - Disable/Enable antivirus protection

`restore` - Restores default settings

ARGUMENTS:

`disabled` - Disable antivirus protection

`enabled` - Enable antivirus protection

EXAMPLES:

`get status` - Shows current protection status

`set status disabled` - Disables protection

`restore status` - Restores protection to default setting (Enabled)

VIRLOG

This is an alias of the `DETECTIONS` command. It is useful when you need to view information about detected infiltrations.

WARNLOG

This is an alias of the `EVENTS` command. It is useful when you need to view information about various events.

4.7.6.3 Batch files / Scripting

You can use eShell as a powerful scripting tool for automation. To use batch file with eShell, create one with an eShell and command in it. For example:

```
eshell get antivirus status
```

You can also chain commands, which is sometimes necessary, for instance if you want to get type of a particular scheduled task, enter the following:

```
eshell select scheduler task 4 "&" get scheduler action
```

Selection of item (task number 4 in this case) usually applies only to a currently running instance of eShell. If you were to run these two commands one after the other, the second command would fail with "No task selected or selected task no longer exist" error.

Due the security reasons, the execution policy is set to Limited Scripting by default. This allows you to use eShell as a monitoring tool, but it won't let you to make configuration changes of ESET Mail Security. Commands that can affect security, such as turning off protection, you will get **Access Denied** message. To be able to execute these commands that make configuration changes we recommend you to use signed batch files.

If, for some specific reason, you need to be able to change configuration using single command entered manually in Windows Command Prompt, then you have to grant eShell full access (not recommended). To grant full access, use `ui eshell shell-execution-policy` command in Interactive mode of eShell itself, or you can do it via GUI in **Advanced Setup** > **User interface** > ESET Shell.

Signed batch files
eShell allows you to secure common batch files (*.bat) with a signature. Scripts are signed with the same password that is used for settings protection. In order to sign a script you need to enable settings protection first. You can do if via GUI, or from within eShell using `set ui access lock-password` command. Once the settings protection password is setup you can start signing batch files.

To sign a batch file, run `sign <script.bat>` from root context of eShell, where *script.bat* is path to the script you want to sign. Enter and confirm password that will be used for signing. This password must match settings protection password. Signature is placed at the end of the batch file in a form of a comment. In case this script has been previously signed, the signature will be replaced with the new one.

NOTE: When you modify previously signed batch file, it needs to be signed again.

NOTE: If you change settings protection password, then you need to sign all scripts again, otherwise the scripts will fail to execute from the moment you've changed settings protection password. This is because the password entered when signing script must match the settings protection password on the target system.

To execute signed batch file from Windows Command Prompt or as a scheduled task, use following command:

```
eshell run <script.bat>
```

Where script.bat is path to the batch file. For example `eshell run d:\myeshellscript.bat`

4.7.7 ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components such as installed drivers and applications, network connections or important registry entries and assesses the risk level of each component. This information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection.

The ESET SysInspector window displays the following information about created logs:

- **Time** - The time of log creation.
- **Comment** - A short comment.
- **User** - The name of the user who created the log.
- **Status** - The status of log creation.

The following actions are available:

- **Open** - Opens created log. Also you can do it by right-clicking the created log and then selecting **Show** from the context menu.
- **Compare** - Compares two existing logs.
- **Create** - Creates a new log. Please wait until the ESET SysInspector log is complete (**Status** shown as Created).
- **Delete** - Removes selected logs from the list.

After right-clicking one or more selected logs, the following options are available from the context menu:

- **Show** - Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Compare** - Compares two existing logs.
- **Create -** Creates a new log. Please wait until the ESET SysInspector log is complete (**Status** shown as Created).
- **Delete** - Removes selected logs from the list.
- **Delete all** - Deletes all logs.
- **Export** - Exports the log to an *.xml* file or zipped *.xml*.

4.7.7.1 Create a computer status snapshot

Enter a short comment describing the log to be created and click the **Add** button. Please wait until the ESET SysInspector log is complete (Status of Created). Log creation may take some time depending on your hardware configuration and system data.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator). For more information see section ESET SysInspector as part of ESET Mail Security.

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

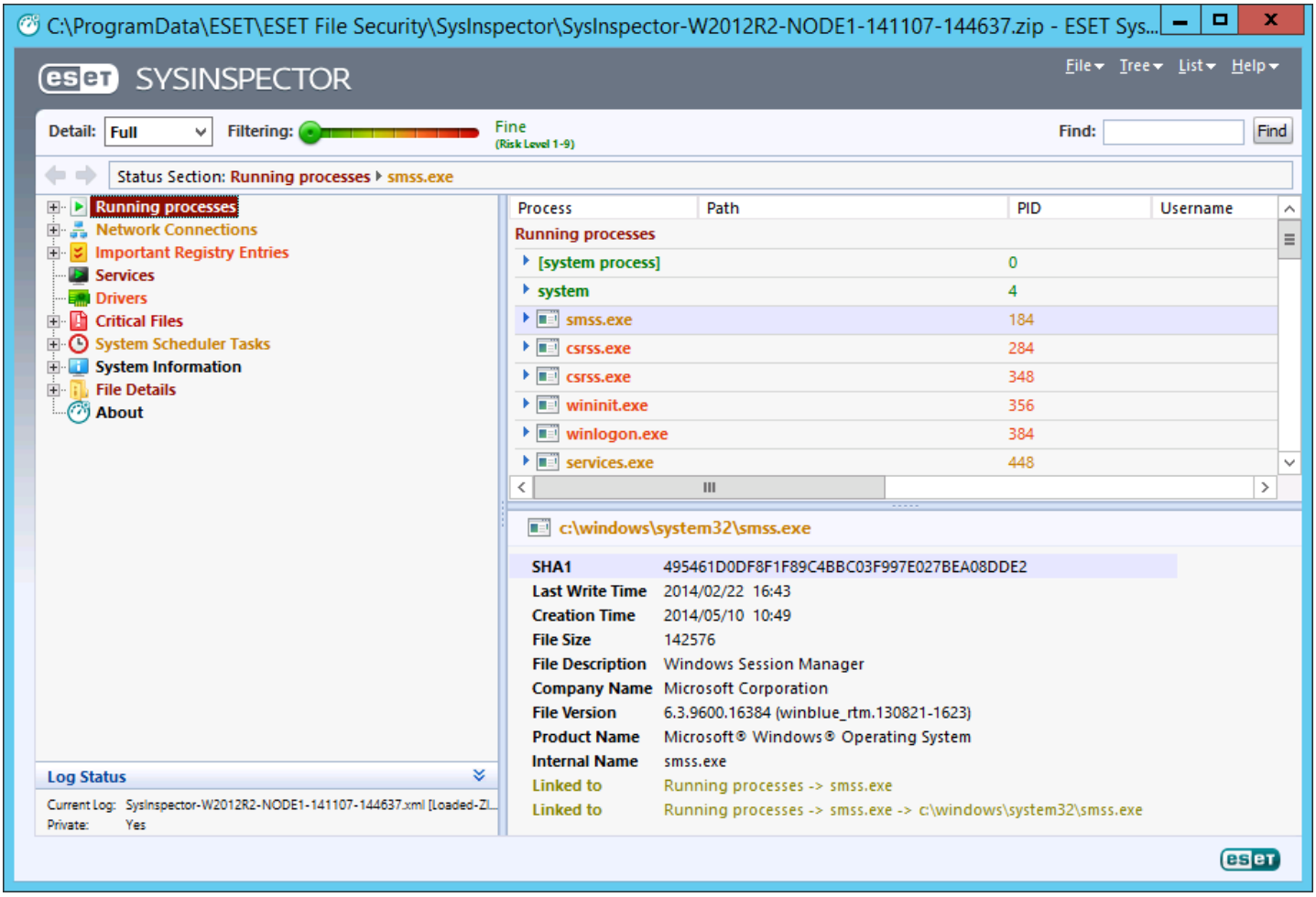
4.7.7.2.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website. If you already have one of the ESET Security solutions installed, you can run ESET SysInspector directly from the Start Menu (click **Programs** > **ESET** > **ESET Mail Security**).

Please wait while the application inspects your system, which could take up to several minutes.

4.7.7.2.2 User Interface and application usage

For clarity the main program window is divided into four major sections – Program Controls located on the top of the main program window, Navigation window to the left, the Description window to the right and the Details window at the bottom of the main program window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



4.7.7.2.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by dragging and dropping them into the main program window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the main program window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current risk level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose a security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the **Risk Level** slider.

Compare

When comparing two logs, you can choose to display all items, display only added items, display only removed items or to display only replaced items.

Find

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return

By clicking the back or forward arrows, you can return to previously displayed information in the Description window. You can use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

4.7.7.2.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or click + or − next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system is comprised of several important kernel components running constantly that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network Connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical Files

The Description window displays content of critical files related to the Microsoft windows operating system.

System Scheduler Tasks

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

System Information

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

File Details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about version of ESET SysInspector and the list of program modules.

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O	opens existing log
Ctrl+S	saves created logs

Generate

Ctrl+G	generates a standard computer status snapshot
Ctrl+H	generates a computer status snapshot that may also log sensitive information

Item Filtering

1, O	fine, risk level 1-9 items are displayed
2	fine, risk level 2-9 items are displayed
3	fine, risk level 3-9 items are displayed
4, U	unknown, risk level 4-9 items are displayed
5	unknown, risk level 5-9 items are displayed
6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+0	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item
Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor
Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field

Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help
Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

4.7.7.2.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Click **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, click **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, click **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

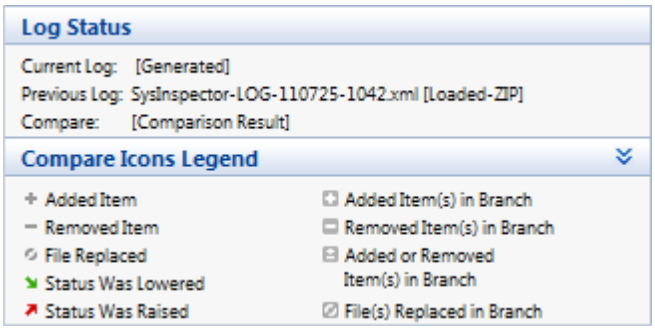
NOTE: If you compare two log files, click **File** > **Save log** to save it as a ZIP file; both files will be saved. If you open this file later, the contained logs are automatically compared.

Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- ▫ tree structure section contains new values
- – removed value, present in the previous log
- ▪ tree structure section contains removed values
- ✎ value / file has been changed
- ▫ tree structure section contains modified values / files
- ↘ the risk level has decreased / it was higher in the previous log
- ↗ the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, click **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

SysIsnpector.exe current.xml previous.xml

4.7.7.2.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen	generate log directly from the command line without running GUI
/privacy	generate log with sensitive information omitted
/zip	save outcome log in compressed zip archive
/silent	suppress progress window when generating log from the command line
/blank	launch ESET SysInspector without generating/loading log

Examples

Usage:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

To load specific log directly into the browser, use: *SysInspector.exe .\clientlog.xml*
To generate log from the command line, use: *SysInspector.exe /gen=.\mynewlog.xml*
To generate log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
To compare two log files and browse differences, use: *SysInspector.exe new.xml old.xml*

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

4.7.7.2.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you suspect that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

1. Run ESET SysInspector to generate a new system snapshot.
2. Select the first item in the section on the left (in the tree structure), press Shift and select the last item to mark all items.
3. Right click the selected objects and select **Export Selected Sections To Service Script**.
4. The selected objects will be exported to a new log.
5. This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
6. Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
7. Click **OK** to run the script.

4.7.7.2.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either **Export All Sections To Service Script** or **Export Selected Sections To Service Script**.

NOTE: It is not possible to export the service script when two logs are being compared.

4.7.7.2.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a “+”. When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependent services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

09) Critical files

This section contains information about files that are critical to proper function of the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

4.7.7.2.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

4.7.7.2.5 FAQ

Does ESET SysInspector require Administrator privileges to run?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file?

ESET SysInspector can create a log file of your computer's configuration. To save one, click **File** > **Save Log** in the main program window. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file?

To view a log file created by ESET SysInspector, run the program and click **File** > **Open Log** in the main program window. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology?

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time?

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%\system32\catroot*) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in *C:\Program Files\Windows NT*. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* pointing to *C:\Program Files\Windows NT\hypertrm.exe* (the main executable of the HyperTerminal application) and *sp4.cat* is digitally signed by Microsoft.

4.7.7.2.6 ESET SysInspector as part of ESET Mail Security

To open the ESET SysInspector section in ESET Mail Security, click **Tools** > **ESET SysInspector**. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To compare, create, or delete snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, select **Show** from the context menu. To export the selected snapshot to a file, right-click it and select **Export...**.

Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.
- **Create...** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.
- **Delete/Delete all** – Removes entries from the list.
- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

4.7.8 ESET SysRescue Live

ESET SysRescue Live is a utility that enables you to create a bootable disk containing one of the ESET Security solutions - ESET NOD32 Antivirus, ESET Smart Security or certain server-oriented products. The main advantage of ESET SysRescue Live is the fact that the ESET Security solution runs independent of the host operating system but has direct access to the disk and file system. This makes it possible to remove infiltrations which normally could not be deleted, for example, when the operating system is running, etc.

4.7.9 Scheduler

Scheduler manages and launches scheduled tasks with predefined configurations and properties. The configuration and properties contain information such as the date and time as well as profiles to be used during the execution of a task.

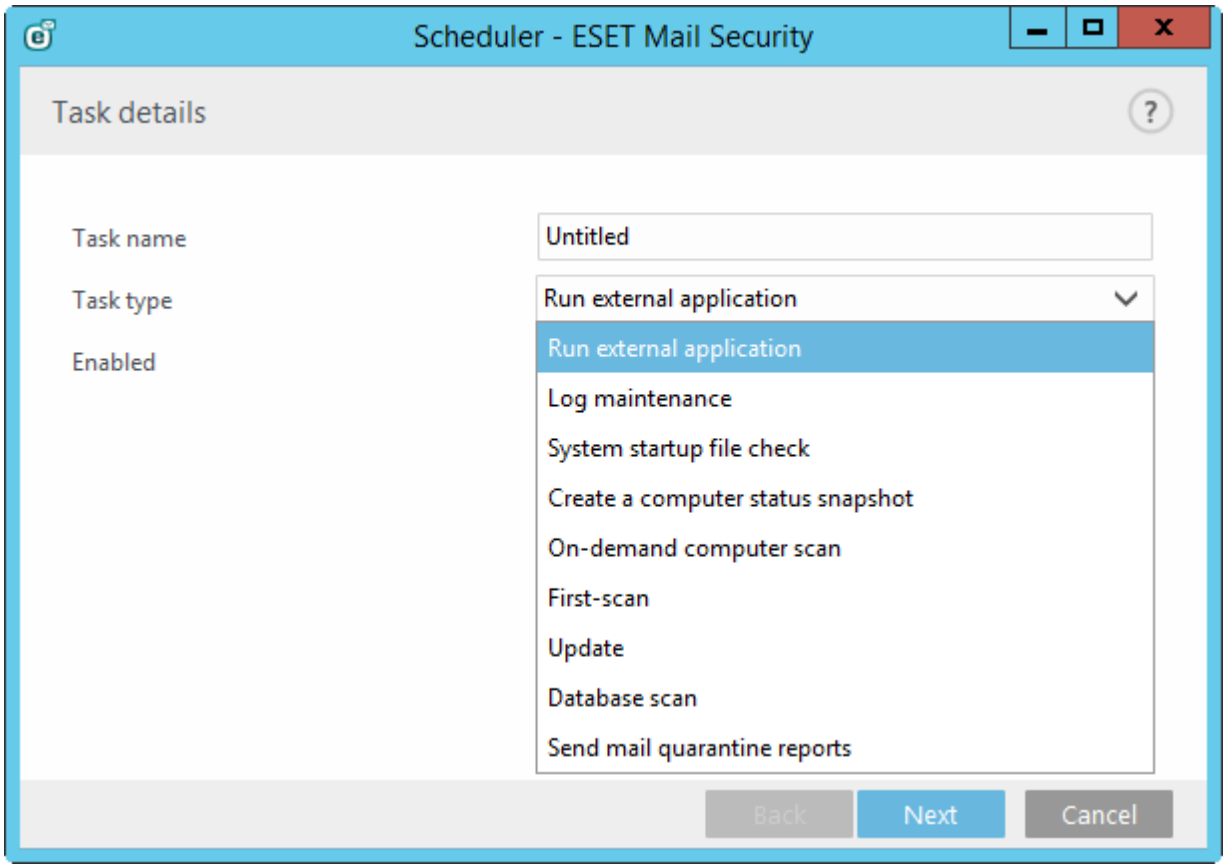
The Scheduler can be accessed from the ESET Mail Security main program window by clicking **Tools** > **Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time and scanning profile used.

The Scheduler serves to schedule the following tasks: virus signature database update, scanning task, system startup file check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add task** or **Delete**). Right-click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, or delete an existing task. Use the check boxes at the beginning of each entry to activate/deactivate the tasks.

By default, the following scheduled tasks are displayed in **Scheduler**:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)
- **Automatic first scan**

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit** or select the task you want to modify and click **Edit**.



Add a new task

1. Click **Add task** at the bottom of the window.
2. Enter a name for the task.
3. Select the desired task from the pull-down menu:

- **Run external application** - Schedules the execution of an external application.
- **Log maintenance** - Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** - Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** - Creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** - Performs a computer scan of files and folders on your computer.
- **First-scan** - By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** - Schedules an Update task by updating the virus signature database and program modules.
- **Database scan** - Schedules database scan, you can select scan targets (Public folders, Databases and Mailboxes) the same way as when configuring On-demand database scan.
- **Send quarantine reports** - Applies to Local quarantine only. Sends reports containing quarantine status and its contents, including links to Mail Quarantine Web interface which allows you to quickly view and manage quarantined email objects. You can specify email address of the recipient for the quarantine reports.

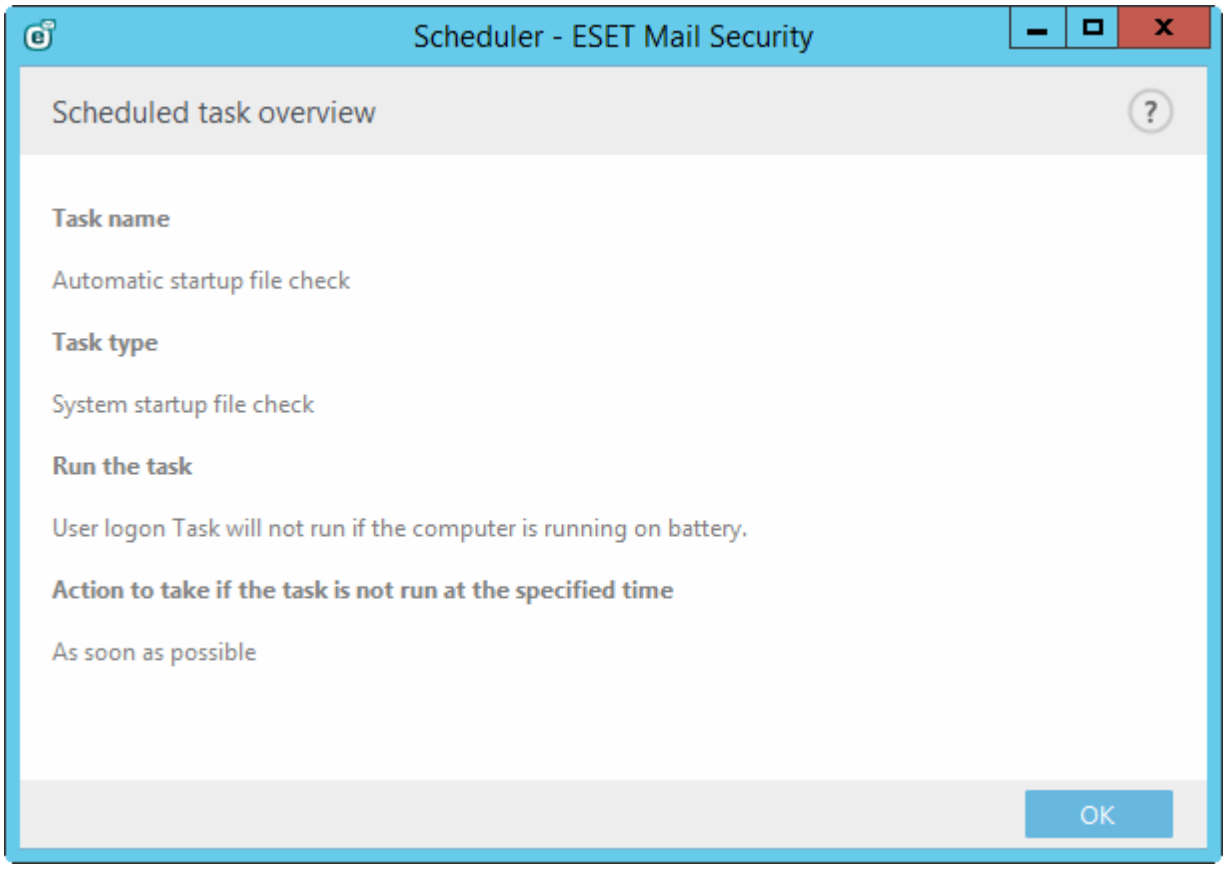
4. Click the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting check box in the list of scheduled tasks), click **Next** and select one of the timing options:

- **Once** - The task will be performed at the predefined date and time.
- **Repeatedly** - The task will be performed at the specified time interval.
- **Daily** - The task will run repeatedly each day at the specified time.
- **Weekly** - The task will be run on the selected day and time.
- **Event triggered** - The task will be performed on a specified event.

5. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. If the task could not be run at the predefined time, you can specify when it will be performed again:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if the time since the last run exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

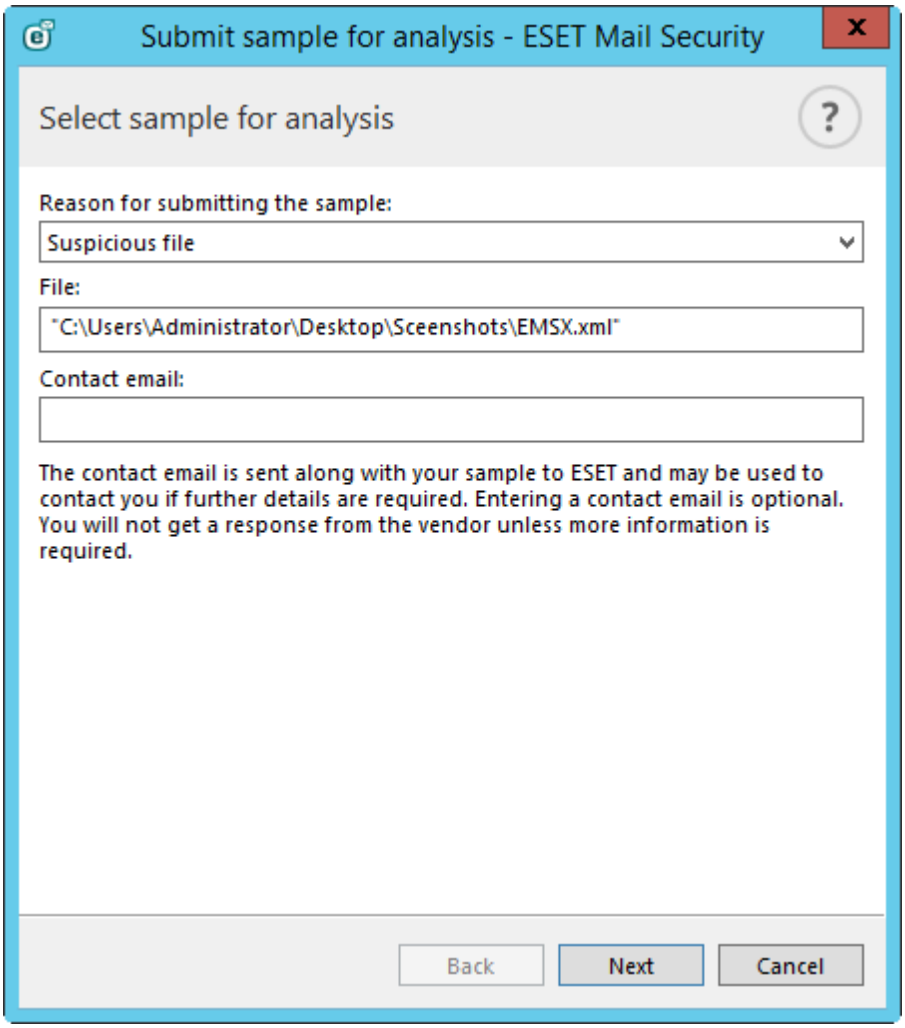
Right-click a task and click **Show task details** from the context menu to view information about the task.


Scheduler - ESET Mail Security
Scheduled task overview
Task name
Automatic startup file check
Task type
System startup file check
Run the task
User logon Task will not run if the computer is running on battery.
Action to take if the task is not run at the specified time
As soon as possible
OK

4.7.10 Submit samples for analysis

The sample submission dialog enables you to send a file or a site to ESET for analysis and can be found in **Tools** > **Submit sample for analysis**. If you find a suspiciously behaving file on your computer or suspicious site on the Internet, you can submit it to the ESET Virus Lab for analysis. If the file turns out to be a malicious application or website, its detection will be added to an upcoming update.

Alternatively, you can submit the file by email. To do so, compress the file(s) using a program like WinRAR or WinZip, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).


Submit sample for analysis - ESET Mail Security
Select sample for analysis
Reason for submitting the sample:
Suspicious file
File:
"C:\Users\Administrator\Desktop\Sceenshots\EMSX.xml"
Contact email:
The contact email is sent along with your sample to ESET and may be used to contact you if further details are required. Entering a contact email is optional. You will not get a response from the vendor unless more information is required.
Back
Next
Cancel

NOTE: Before submitting a sample to ESET, make sure it meets one or more of the following criteria:

- the file or website is not detected at all
- the file or website is incorrectly detected as a threat

You will not receive a response unless further information is required for analysis.

Select the description from the **Reason for submitting the sample** drop-down menu that best fits your message:

- **Suspicious file**
- **Suspicious site** (a website that is infected by any malware)
- **False positive file** (file that is detected as an infection but are not infected)
- **False positive site**
- **Other**

File/Site - The path to the file or website you intend to submit.

Contact email - This contact email is sent along with suspicious files to ESET, and may be used to contact you if further information is required for analysis. Entering a contact email is optional. You will not get a response from ESET unless more information is required; since each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.

4.7.10.1 Suspicious file

Observed signs and symptoms of malware infection - Enter a description of the suspicious file behavior observed on your computer.

File origin (URL address or vendor) - Please enter the file origin (source) and how you encountered this file.

Notes and additional information - Here you can enter additional info or a description that will help with the process of identifying the suspicious file.

NOTE: The first parameter - **Observed signs and symptoms of malware infection** - is required, but providing additional information will significantly help our laboratories with the identification process of samples.

4.7.10.2 Suspicious site

Please select one of the following from the **What's wrong with the site** drop-down menu:

- **Infected** - A website that contains viruses or other malware distributed by various methods.
- **Phishing** - Often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this type of attack in the glossary.
- **Scam** - A swindle or a fraudulent website.
- Select **Other** if the aforementioned options do not refer the site you are going to submit.

Notes and additional information - Here you can enter additional info or a description that will help while analyzing the suspicious website.

4.7.10.3 False positive file

We request that you submit files that are detected as an infection but are not infected to improve our antivirus and antispyware engine and help others to be protected. False positives (FP) may occur when a pattern of a file matches the same pattern contained in a virus signature database.

Application name and version - Program title and its version (for example number, alias or code name).

File origin (URL address or vendor) - Please enter a file origin (source) and note how you encountered this file.

Application's purpose - The general application description, type of application (e.g. browser, media player, ...) and its functionality.

Notes and additional information - Here you can add additional information or descriptions that will help while processing the suspicious file.

NOTE: The first three parameters are required to identify legitimate applications and distinguish them from malicious code. By providing additional information, you will help our laboratories significantly in the identification process and in the processing of samples.

4.7.10.4 False positive site

We encourage you to submit sites that are detected as an infected, scam or phishing sites but are not. False positives (FP) may occur when a pattern of a file matches the same pattern contained in a virus signature database. Please provide this website to improve our antivirus and anti-phishing engine and help others to be protected.

Notes and additional information - Here you can add additional information or descriptions that will help while processing the suspicious file.

4.7.10.5 Other

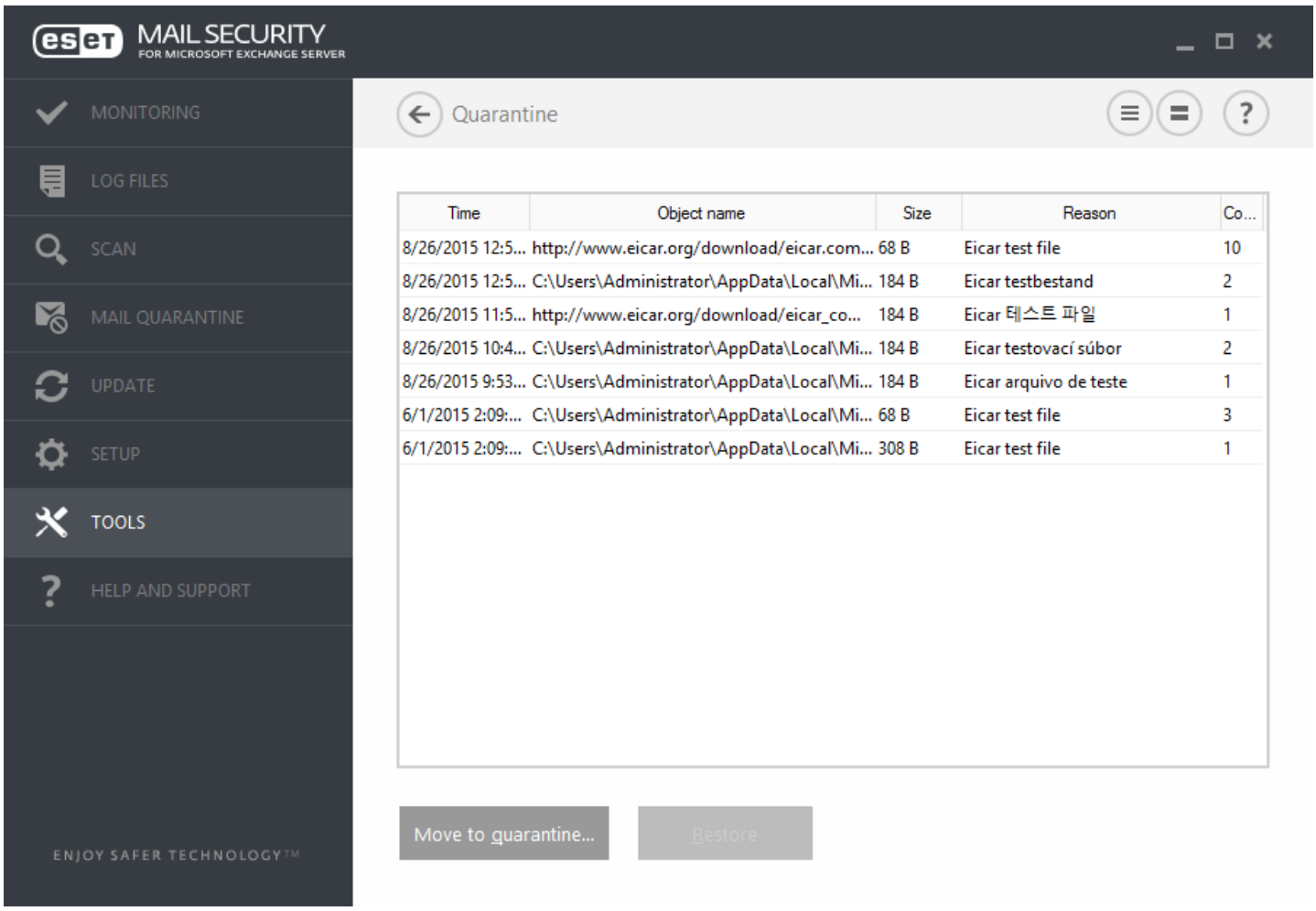
Use this form if the file cannot be categorized as a **Suspicious file** or as a **False positive**.

Reason for submitting the file - Please enter a detailed description and the reason for sending the file.

4.7.11 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET Mail Security.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.



Files stored in the quarantine folder can be viewed in a table that displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (for example, object added by user), and number of threats (for example, if it is an archive containing multiple infiltrations).

In case email message objects are quarantined in the file quarantine, information in a form of path to the mailbox/ folder/filename is displayed.

Quarantining files

ESET Mail Security automatically quarantines deleted files (if you have not disabled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Quarantine.** Quarantined files will be removed from their original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine**.

Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature, available from the context menu by right-clicking a given file in the Quarantine window, to do so. If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option will be available. Read more about this type of application in the glossary. The context menu also offers the **Restore to...** option which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantines a harmless file by mistake, please exclude the file from scanning after restoring it and send the file to ESET Customer Care.

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

4.8 Help and support

ESET Mail Security contains troubleshooting tools and support information that will assist you in solving issues that you may encounter.

Help

- **Search ESET Knowledgebase** - The ESET Knowledgebase contains answers to the most frequently asked questions as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- **Open help** - Click this link to launch the ESET Mail Security help pages.
- **Find quick solution** - Select this to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting technical support.

Customer Care

- **Submit support request** - If you could not find an answer to your problem, you can also use this form located on the ESET website to quickly contact our Customer Care department.

Support Tools

- **Threat encyclopedia -** Links to the ESET Threat Encyclopedia, which contains information about the dangers and symptoms of different types of infiltration.
- **Virus signature database history** - Links to ESET Virus radar, which contains information about versions of the ESET Virus signature database.
- **ESET Specialized cleaner** - This cleaner automatically identifies and removes common malware infections, for more information please visit this ESET Knowledgebase article.

Product and License information

- **About ESET Mail Security -** Displays information about your copy of ESET Mail Security.
- Manage license - Click to launch the Product activation window. Select one of the available methods to activate ESET Mail Security. See How to activate ESET Mail Security for more information.

4.8.1 How to

This chapter covers some of the most frequently asked questions and problems encountered. Click the topic title to find out how to solve your problem:

How to update ESET Mail Security

How to activate ESET Mail Security

How to schedule a scan task (every 24 hours)

How to remove a virus from my server

How Automatic exclusions work

If your problem is not included in the help pages list above, try searching by keyword or phrase describing your problem and search within the ESET Mail Security Help Pages.

If you cannot find the solution to your problem/question within the Help Pages, you can try our regularly updated online Knowledgebase.

If necessary, you can directly contact our online technical support center with your questions or problems. The contact form can be found in the **Help and Support** tab of your ESET program.

4.8.1.1 How to update ESET Mail Security

Updating ESET Mail Security can be performed either manually or automatically. To trigger the update, click **Update virus signature database**. You will find this in the **Update** section of the program.

The default installation settings create an automatic update task which is performed on an hourly basis. If you need to change the interval, navigate to the **Scheduler** (for more information on Scheduler, click here).

4.8.1.2 How to activate ESET Mail Security

After installation is complete, you will be prompted to activate your product.

There are several methods for activating your product. Availability of a particular activation scenario in the activation window may vary depending on the country, as well as the means of distribution (CD/DVD, ESET web page, etc.).

To activate your copy of ESET Mail Security directly from the program, click the system tray icon and select **Activate product license** from the menu. You can also activate your product from the main menu under **Help and support** > **Activate License** or **Protection status** > **Activate product license**.

You can use any of the following methods to activate ESET Mail Security:

- **License Key** - A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and for activation of the license.
- **Security Admin account** - An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline License file** - An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the license portal and is used in environments where the application cannot connect to the licensing authority.

Click **Activate later** with ESET Remote Administrator if your computer is a member of a managed network, and your administrator will perform remote activation via ESET Remote Administrator.You can also use this option if you want to activate this client at a later time.

Click **Help and support** > **Manage license** in the main program window to manage your license information at any time. You will see the public license ID used to identify your product by ESET and for license identification. Your Username, under which the computer is registered with licensing system, is stored in the **About** section, which you can view by right-clicking the system tray icon .

NOTE: ESET Remote Administrator is able to activate client computers silently using licenses made available by

the administrator.

4.8.1.3 How does ESET Mail Security count mailboxes

For details see our Knowledgebase article.

4.8.1.4 How to create a new task in Scheduler

To create a new task in **Tools** > **Scheduler**, click **Add task** or right-click and select **Add** from the context menu. Five types of scheduled tasks are available:

- **Run external application** - Schedules the execution of an external application.
- **Log maintenance** - Log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** - Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** - Creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** - Performs a computer scan of files and folders on your computer.
- **First scan** - By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** - Schedules an Update task by updating the virus signature database and program modules.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:

From the **Scheduled task** drop-down menu, select **Update**. Enter the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered.** Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if time since last run exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

4.8.1.5 How to schedule a scan task (every 24 hours)

To schedule a regular task, go to **ESET Mail Security** > **Tools** > **Scheduler**. Below, you can find a short guide on how to schedule a task that will scan your local drives every 24 hours.

To schedule a scan task:

1. Click **Add** in the main Scheduler screen.
2. Select **On-demand computer scan** from the drop-down menu.
3. Enter a name for the task and select **Repeatedly**.
4. Choose to run the task every 24 hours (1440 minutes).
5. Select an action to perform if the scheduled task execution fails for any reason.
6. Review the summary of the scheduled task and click **Finish**.
7. From the **Targets** drop-down menu, select Local drives.
8. Click **Finish** to apply the task.

4.8.1.6 How to remove a virus from your server

If your computer is showing symptoms of malware infection, for example, it is slower or often freezes, we recommend that you do the following:

1. From the main ESET Mail Security window, click **Computer scan**.
2. Click **Smart scan** to begin scanning your system.
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.
4. If you want to only scan a certain part of your disk, choose **Custom scan** and select targets to be scanned for viruses.

4.8.2 Submit support request

In order to provide assistance as quickly and accurate as possible, ESET requires information about your ESET Mail Security configuration, detailed system system information and running processes (ESET SysInspector log file) and registry data. ESET will only use this data to provide technical assistance to the customer.

When you submit the web form, your system configuration data will be submitted to ESET. Select **Always submit this information** if you want to remember this action for this process. To submit the form without sending any data click **Don't submit data** and you can contact ESET customer care using the online support form.

This setting can also be configured in **Advanced setup** > **Tools** > **Diagnostics** > **Customer Care**.

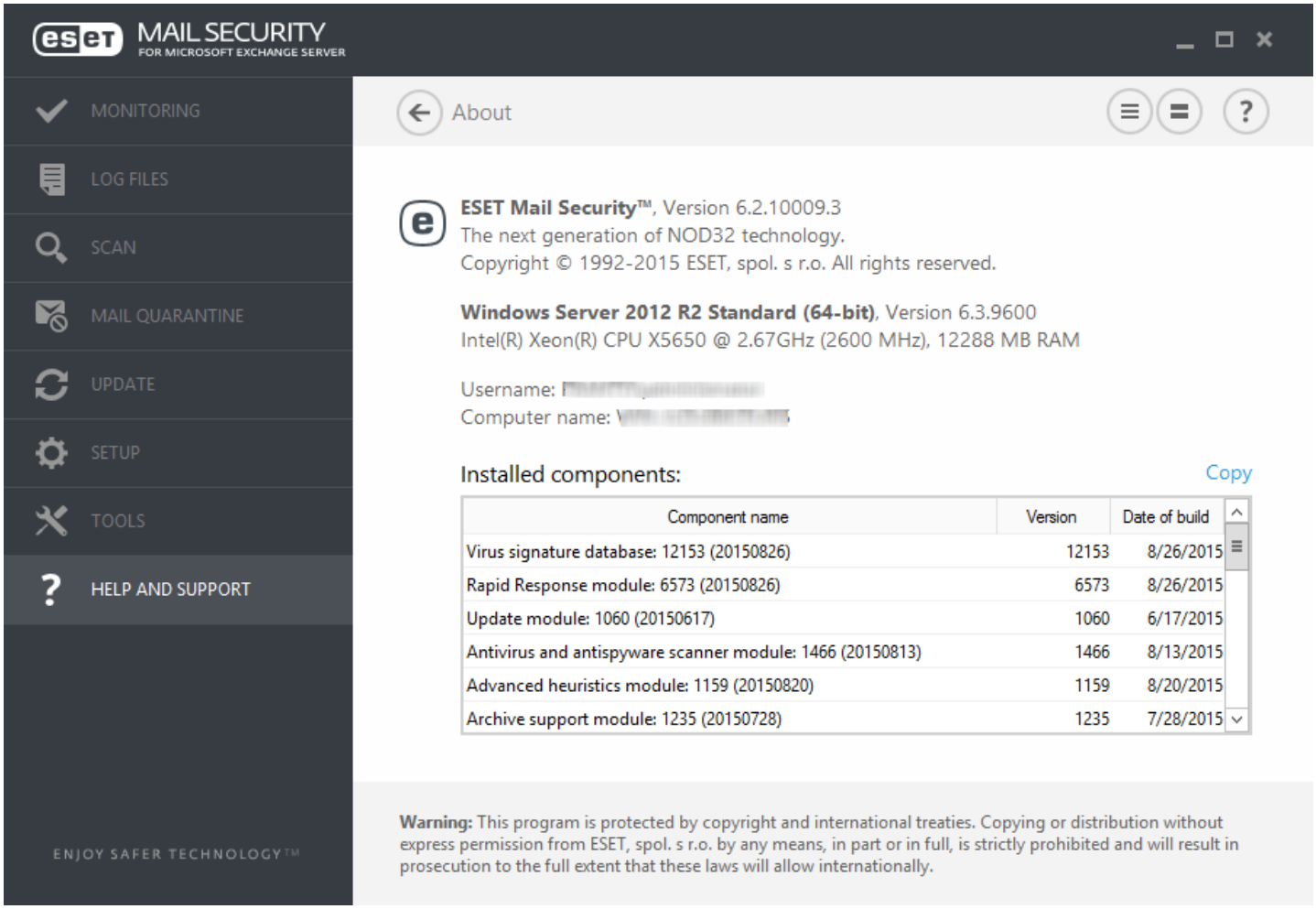
NOTE: If you have decided to submit system data it is needed to fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.

4.8.3 ESET Specialized Cleaner

The ESET Specialized Cleaner is a removal tool for common malware infections such as Conficker, Sirefef or Necurs. For more information please visit this ESET Knowledgebase article.

4.8.4 About ESET Mail Security

This window provides details about installed version of ESET Mail Security and the list of installed program modules. The top part of the window contains information about your operating system and system resources.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
MONITORING
LOG FILES
SCAN
MAIL QUARANTINE
UPDATE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
About
ESET Mail Security™, Version 6.2.10009.3
The next generation of NOD32 technology.
Copyright © 1992-2015 ESET, spol. s r.o. All rights reserved.
Windows Server 2012 R2 Standard (64-bit), Version 6.3.9600
Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2600 MHz), 12288 MB RAM
Username:
Computer name:
Installed components:
Copy
Component name
Version
Date of build
Virus signature database: 12153 (20150826) 12153 8/26/2015
Rapid Response module: 6573 (20150826) 6573 8/26/2015
Update module: 1060 (20150617) 1060 6/17/2015
Antivirus and antispyware scanner module: 1466 (20150813) 1466 8/13/2015
Advanced heuristics module: 1159 (20150820) 1159 8/20/2015
Archive support module: 1235 (20150728) 1235 7/28/2015
Warning: This program is protected by copyright and international treaties. Copying or distribution without express permission from ESET, spol. s r.o. by any means, in part or in full, is strictly prohibited and will result in prosecution to the full extent that these laws will allow internationally.

You can copy information about modules (**Installed components**) to the clipboard by clicking **Copy**. This may be useful during troubleshooting or when contacting Technical Support.

4.8.5 Product activation

After installation is complete, you will be prompted to activate your product.

There are several methods for activating your product. Availability of a particular activation scenario in the activation window may vary depending on the country, as well as the means of distribution (CD/DVD, ESET web page, etc.).

To activate your copy of ESET Mail Security directly from the program, click the system tray icon and select **Activate product license** from the menu. You can also activate your product from the main menu under **Help and support** > **Activate License** or **Protection status** > **Activate product license**.

You can use any of the following methods to activate ESET Mail Security:

- **License Key** - A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and for activation of the license.
- **Security Admin account** - An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline License file** - An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the license portal and is used in environments where the application cannot connect to the licensing authority.

Click **Activate later** with ESET Remote Administrator if your computer is a member of a managed network, and your administrator will perform remote activation via ESET Remote Administrator.You can also use this option if you want to activate this client at a later time.

Click **Help and support** > **Manage license** in the main program window to manage your license information at any time. You will see the public license ID used to identify your product by ESET and for license identification. Your Username, under which the computer is registered with licensing system, is stored in the **About** section, which you can view by right-clicking the system tray icon .

NOTE: ESET Remote Administrator is able to activate client computers silently using licenses made available by the administrator.

4.8.5.1 Registration

Please register your license by completing the fields contained in the registration form and clicking **Continue**. The fields marked as required in brackets are mandatory. This information will only be used for matters involving your ESET License.

4.8.5.2 Security Admin activation

The Security Admin account is an account created on the license portal with your **email address** and **password**, which is able to see all seat authorizations.

A **Security Admin** account allows you to manage multiple licenses. If you do not have a Security Admin account, click **Create account** and you will be redirected to the ESET License Administrator web page where you can register with your credentials.

If you have forgotten your password click **Forgotten password?** and you will be redirected to the ESET Business portal. Enter your email address and click **Submit** to confirm. After that you will obtain a message with instructions to reset your password.

NOTE: For more information about using ESET License Administrator, see the ESET License Administrator User Guide.

4.8.5.3 Activation failure

Activation of ESET Mail Security was not successful. Make sure you have entered the proper **License Key** or attached an **Offline License**. If you have a different **Offline License**, please enter it again. To check the license key you entered, click **recheck the License Key** or click **purchase a new license** and you will be redirected to our webpage where you can buy a new license.

4.8.5.4 License

If you choose the **Security Admin** activation option, you will be prompted to select a license associated with your account that will be used for ESET Mail Security. Click **Activate** to continue.

4.8.5.5 Activation progress

ESET Mail Security is now activating, please be patient. This may take a few moments.

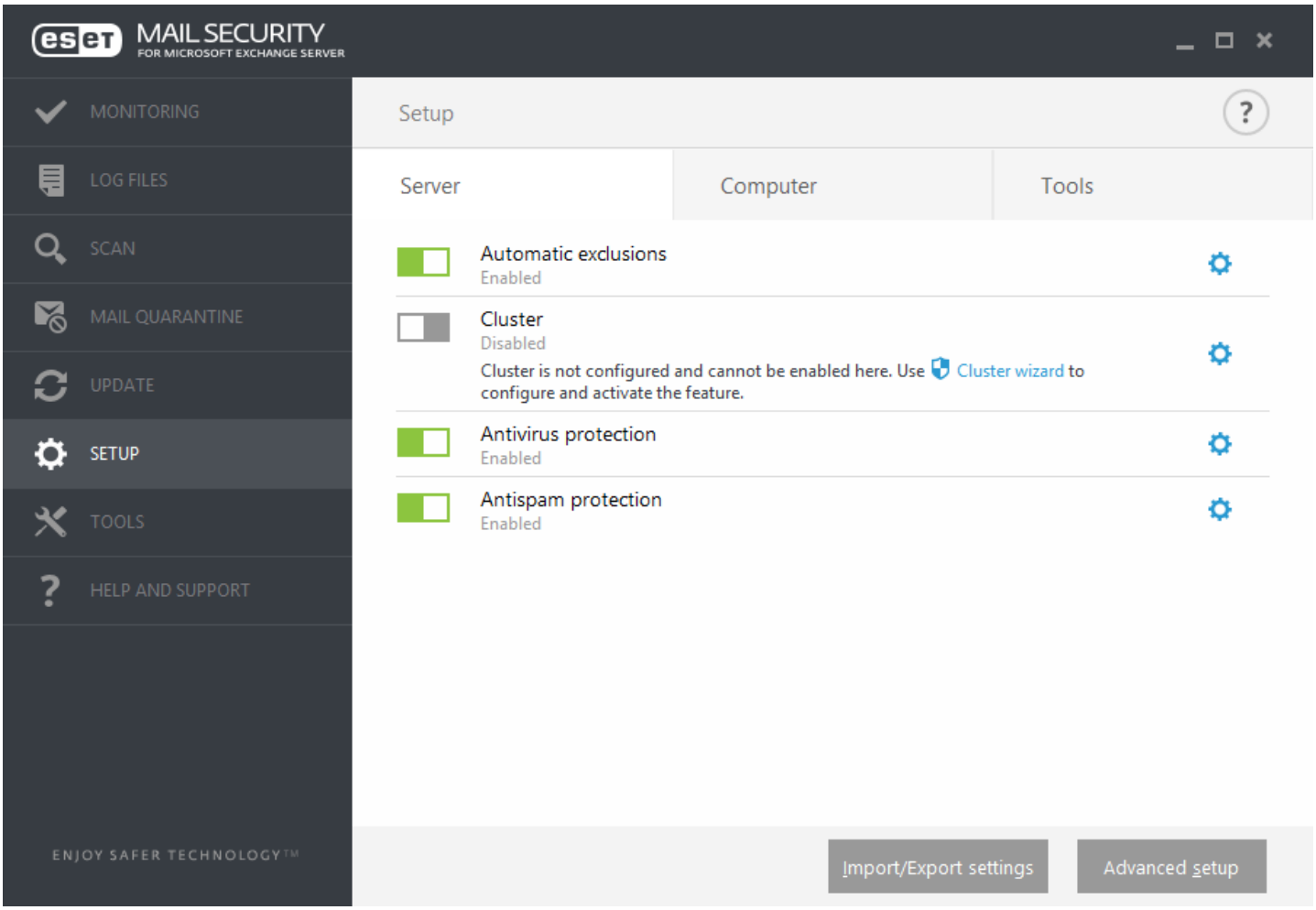
4.8.5.6 Activation successful

Activation was successful and ESET Mail Security is now activated. From now on, ESET Mail Security will receive regular updates to identify the latest threats and keep your computer safe. Click **Done** to finish product activation.

5. Working with ESET Mail Security

The **Setup** menu contains the following sections between which you can switch using tabs:

- Server
- Computer
- Tools



To temporarily disable individual modules, click the green switch next to the desired module. Note that this may decrease the protection level of your computer.
To re-enable the protection of a disabled security component, click the red switch to return a component to its enabled state.
To access detailed settings for a particular security component, click the gear wheel .

Click **Advanced setup** or press **F5** to access additional component settings and options.

There are additional options at the bottom of the setup window. Use **Import/Export settings** to load setup parameters using an *.xml* configuration file, or to save the current setup parameters to a configuration file. See Import/Export settings for more detailed information.

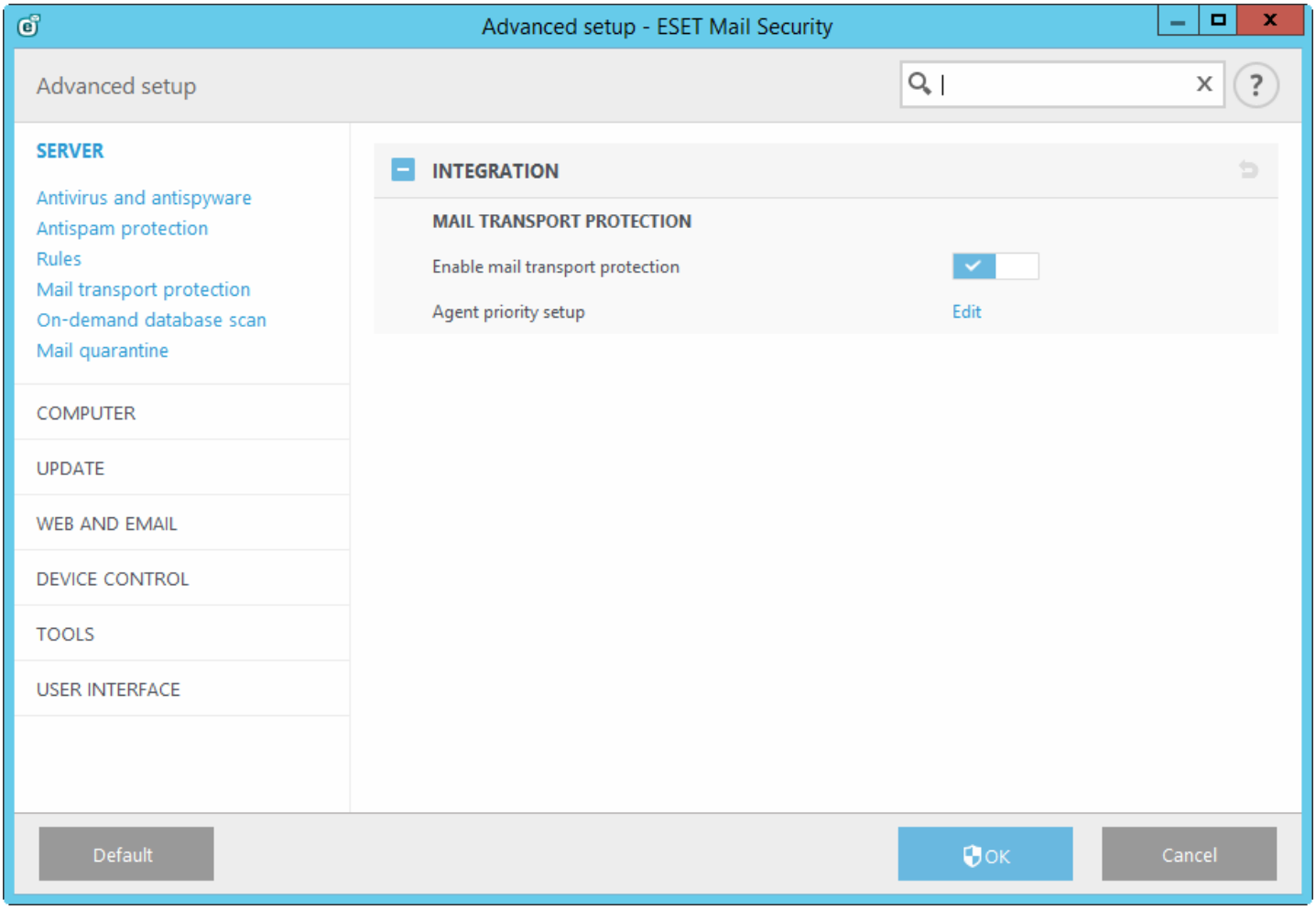
5.1 Server

ESET Mail Security provides significant protection for your Microsoft Exchange Server using the following features:

- Antivirus and antispyware
- Antispam protection
- Rules
- Mail transport protection (Exchange Server 2007, 2010, 2013)
- Mailbox database protection (Exchange Server 2003, 2007, 2010)
- On-demand database scan (Exchange Server 2007, 2010, 2013)
- Quarantine (Mail Quarantine type settings)

This Advanced setup section allows you to enable or disable integration of Mailbox database protection and Mail transport protection as well as edit Agent priority.

NOTE: If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Mailbox database protection and On-demand database scan. However, only one protection type out of these two can be active at a time. If you decide to use On-demand database scan you'll need to disable integration of Mailbox database protection. Otherwise On-demand database scan will not be available.



5.1.1 Agent priority setup

In the **Agent priority setup** menu, you can set the priority in which ESET Mail Security Agents become active after the Microsoft Exchange Server has started. Numeric value defines the priority. The lower the number, the higher the priority. This applies to Microsoft Exchange 2003.

Click **Edit** button to enter Agent priority setup, you can set the priority in which ESET Mail Security Agents become active after the Microsoft Exchange Server has started.

- **Modify** – manually define number to change the priority of a selected Agent.
- **Move up** – increase the priority of a selected Agent by moving it up in the list of Agents.
- **Move down** – decrease the priority of a selected Agent by moving it down in the list of Agents.

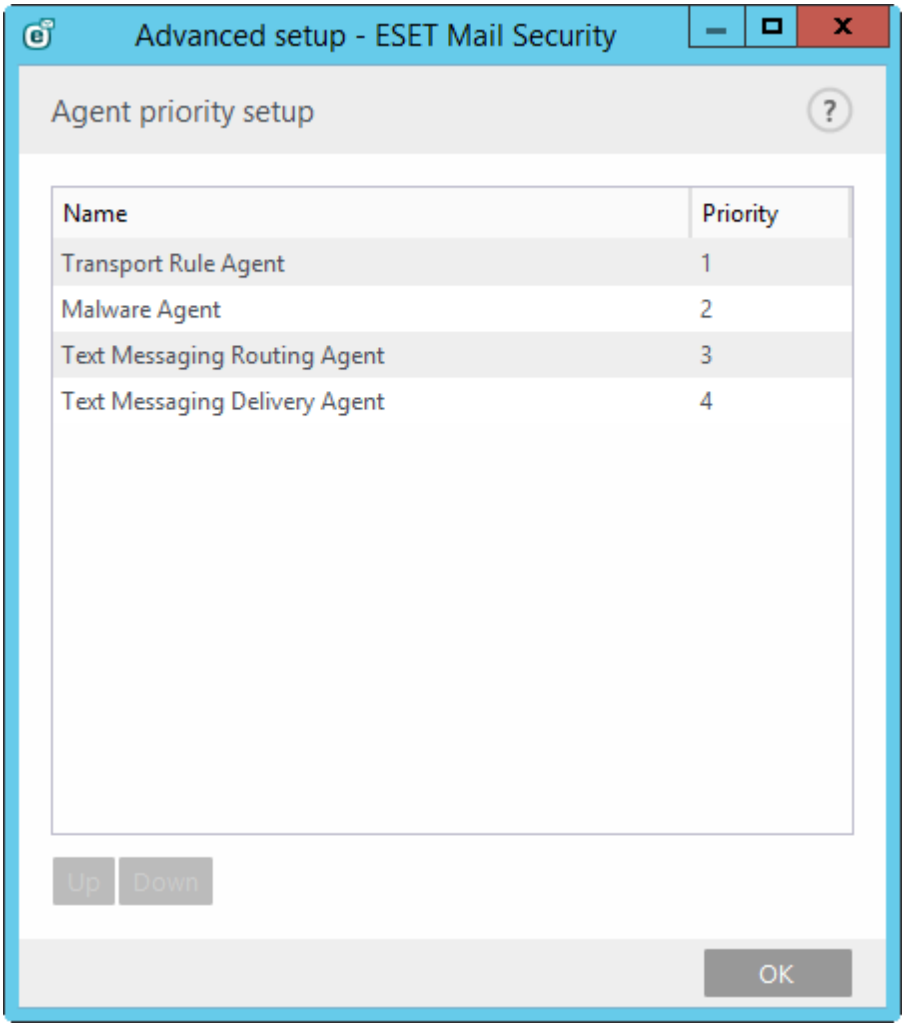
With Microsoft Exchange Server 2003, you can specify Agent priority independently using tabs for EOD (end of data) and RCPT (recipient).

5.1.1.1 Modify priority

If you are running Microsoft Exchange Server 2003, you can manually define number to change the **Priority of transport agent**. Modify the number in the text field or use up and down arrows to change the priority. The lower the number, the higher the priority.

5.1.2 Agent priority setup

In the **Agent priority setup** menu, you can set the priority in which ESET Mail Security Agents become active after the Microsoft Exchange Server has started. This applies to Microsoft Exchange 2007 and newer.



- **Move up** - increase the priority of a selected Agent by moving it up in the list of Agents.

- **Move down -** decrease the priority of a selected Agent by moving it down in the list of Agents.

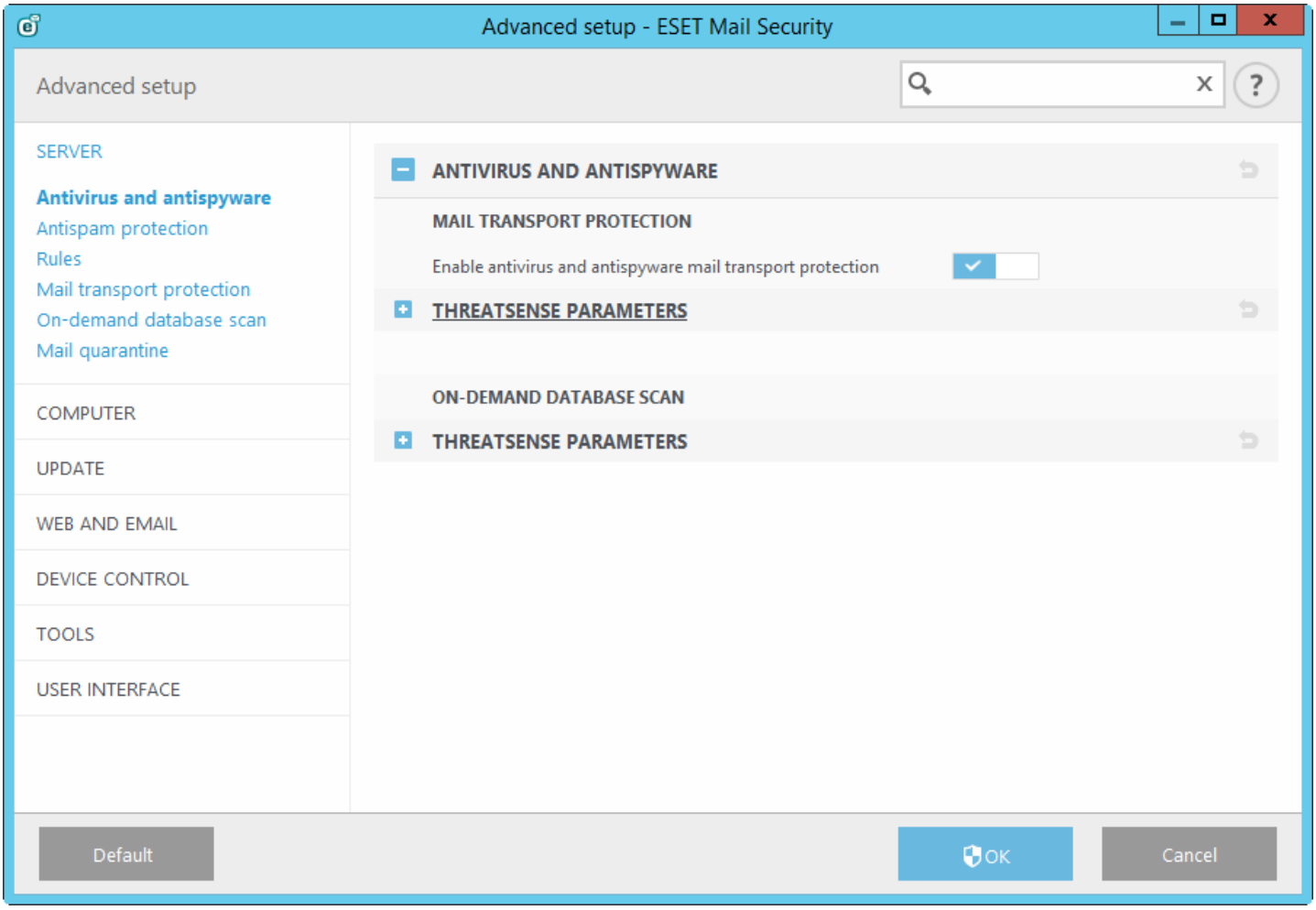
5.1.3 Antivirus and antispyware

In this section you can configure **Antivirus and antispyware** options for your mail server.

IMPORTANT: Mail transport protection is provided by transport agent and is only available for Microsoft Exchange Server 2007 and later, but your Exchange Server must have the Edge Transport Server or Hub Transport Server role. This also applies to a single server installation with multiple Exchange Server roles on one computer (as long as it has the Edge or Hub Transport role).

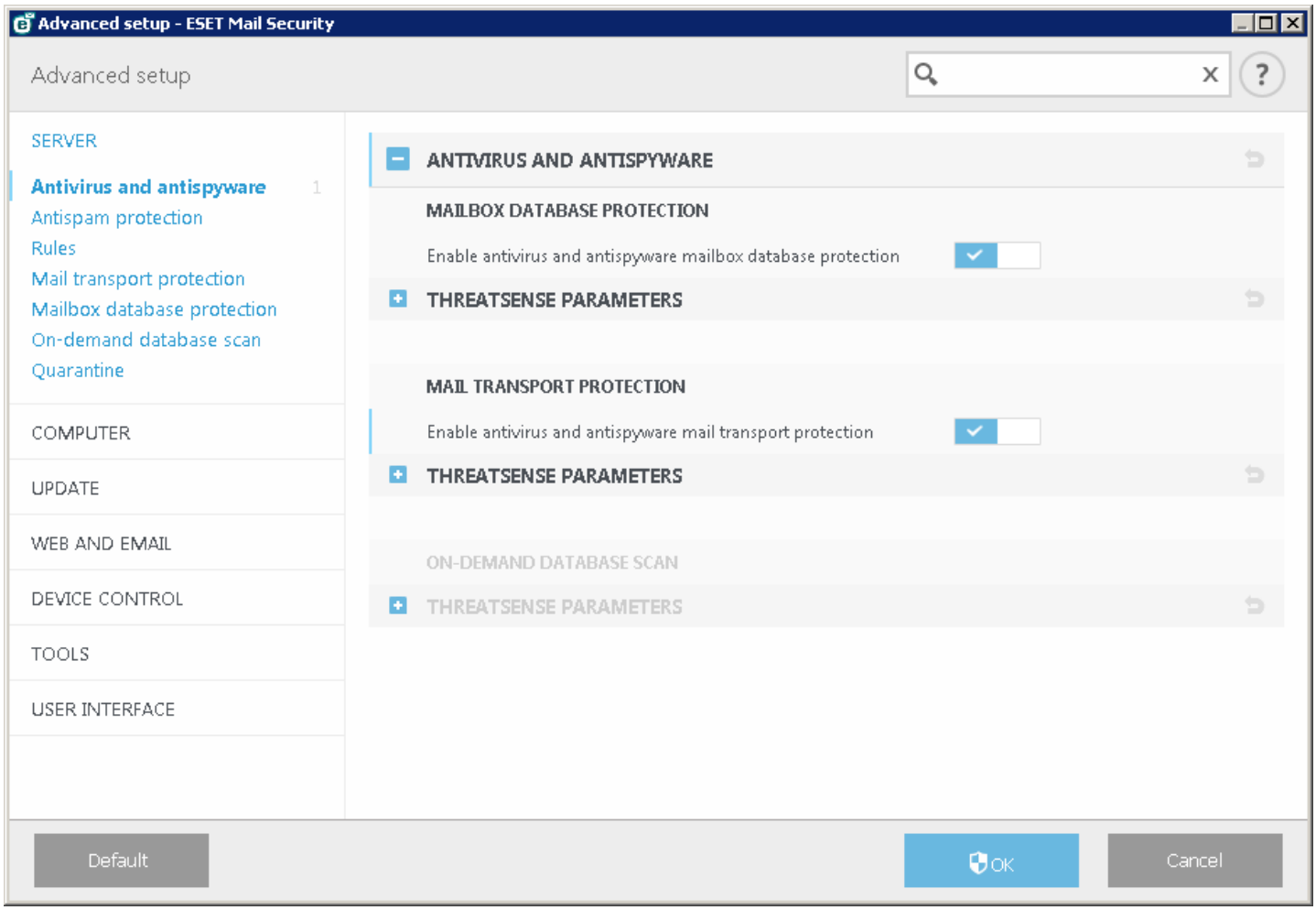
Mail transport protection:

If you disable **Enable antivirus and antispyware mail transport protection**, the ESET Mail Security plug-in for Exchange server will not be unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses on the transport layer. Messages will still be scanned for viruses and spam on the database layer and existing rules will be applied.



Mailbox database protection:

If you disable **Enable antivirus and antispyware mailbox database protection**, the ESET Mail Security plug-in for Exchange server will not be unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses on database layer. Messages will still be scanned for viruses and spam on the transport layer and existing rules will be applied.



5.1.4 Antispam protection

Antispam protection for your mail server is enabled by default. To turn it off, click the switch next to **Enable antispam protection**.

NOTE: Disabling Antispam protection will not change the protection status. Even though the Antispam is disabled, you'll see the green **Maximum protection** is still displayed in the **Monitoring** section of the main GUI. Disabled Antispam is not considered a reduction in protection level.

Enabling **Use Exchange Server whitelists to automatically bypass antispam protection** lets ESET Mail Security use specific Exchange "whitelists". When enabled, the following is taken into consideration:

- The server IP address is on the Allowed IP list of the Exchange Server
- The message recipient has the Antispam Bypass flag set on his/her mailbox
- The message recipient has the sender's address on their Safe Senders List (make sure you have configured Safe Senders List Synchronization within your Exchange Server environment including Safelist Aggregation)

If any of the above applies to an incoming message, the antispam check will be bypassed for this message, the message will not be evaluated for SPAM and will be delivered to the recipient's mailbox.

The **Accept antispam bypass flag set on SMTP session** is useful when you have authenticated SMTP sessions between Exchange Servers with antispam bypass setting. For example, when you have an Edge server and a Hub server, there is no need to scan the traffic between the two servers. The **Accept antispam bypass flag set on SMTP session** is enabled by default but only applies when the antispam bypass flag is configured for the SMTP session on your Exchange Server. If you disable **Accept antispam bypass flag set on SMTP session**, ESET Mail Security will scan the SMTP session for spam regardless of antispam bypass setting on your Exchange Sever.

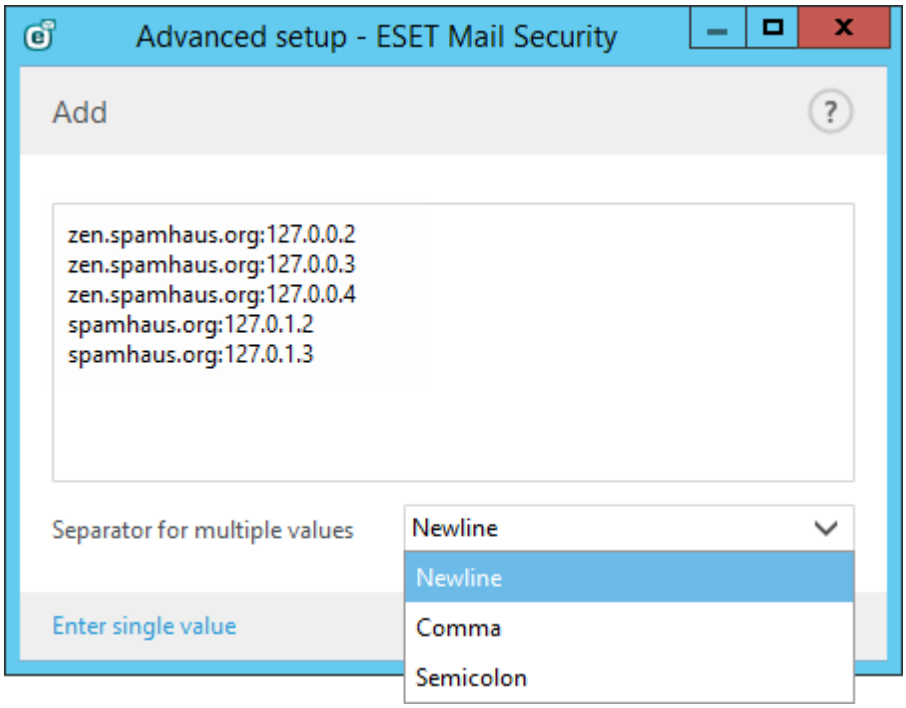
NOTE: It is necessary that the Antispam database be updated regularly for the Antispam module to provide the best possible protection. To allow regular updates to the Antispam database, make sure that ESET Mail Security has access to the correct IP addresses on the necessary ports. For further information on what IPs and ports to enable on your third-party firewall, see our KB article.

5.1.4.1 Filtering and verification

You can configure **Allowed**, **Blocked** and **Ignored** lists by specifying criteria such as IP address or range, domain name, etc. To add, modify or remove criteria, click **Edit** for to the list you want to manage.

- **Approved IP list** - automatically whitelists e-mails originating from specified IP addresses.
- **Blocked IP list** - automatically blocks e-mails originating from specified IP addresses.
- **Ignored IP list** - list of IP addresses which will be ignored during classification.
- **Blocked Body Domain list** - blocks e-mail messages that contain specified domain in the message body.
- **Ignored Body Domain list** - specified domains in the message body will be ignored during classification.
- **Blocked Body IP list** - blocks e-mail messages that contain specified IP address in the message body.
- **Ignored Body IP list** - specified IP addresses in the message body will be ignored during classification.
- **Approved Senders list** - whitelists e-mails originating from specified sender.
- **Blocked Senders list** - blocks e-mails originating from specified sender.
- **Approved Domain to IP list** - whitelists e-mails originating from IP addresses that are resolved from specified domains in this list. SPF (Sender Policy Framework) records are being recognized when resolving IP addresses.
- **Blocked Domain to IP list** - blocks e-mails originating from IP addresses that are resolved from specified domains in this list. SPF records are being recognized when resolving IP addresses.
- **Ignored Domain to IP list** - list of domains that resolves to IP addresses which in turn will not be checked during classification. SPF records are being recognized when resolving IP addresses.
- **Blocked charsets list** - blocks e-mails in specified character sets.
- **Blocked countries list** - blocks e-mails from specified countries.

NOTE: If you want to add more entries at once, click **Enter multiple values** in the Add pop-up window and choose what separator should be used, it can be **Newline**, **Comma** or **Semicolon**. For example:



5.1.4.2 Advanced settings

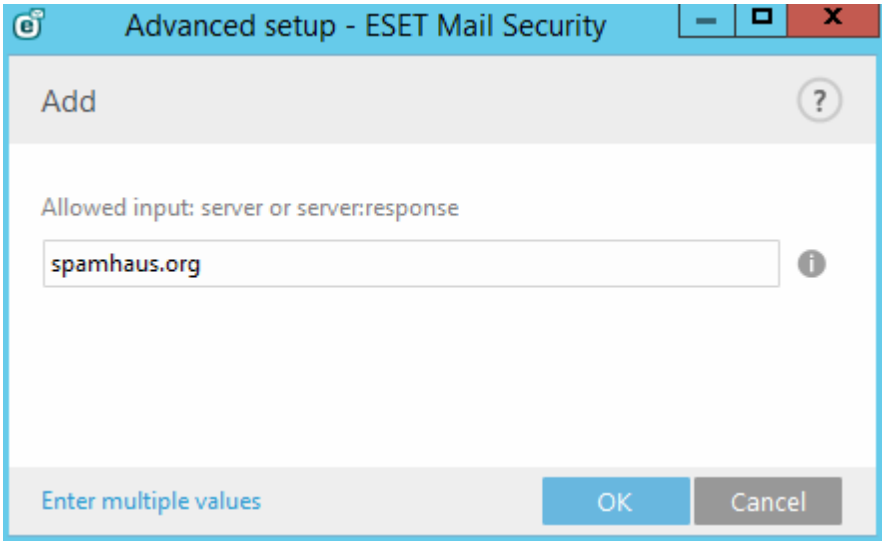
These settings allow for messages to be verified by external servers (**RBL** - Realtime Blackhole List, **DNSBL** - DNS Blocklist) according to defined criteria.

Maximum number of verified addresses from Received: headers. - You can limit the number of IP addresses that are checked by antispam. This concerns the IP addresses written in `Received: from` headers. Default value is 0 which is no limit.

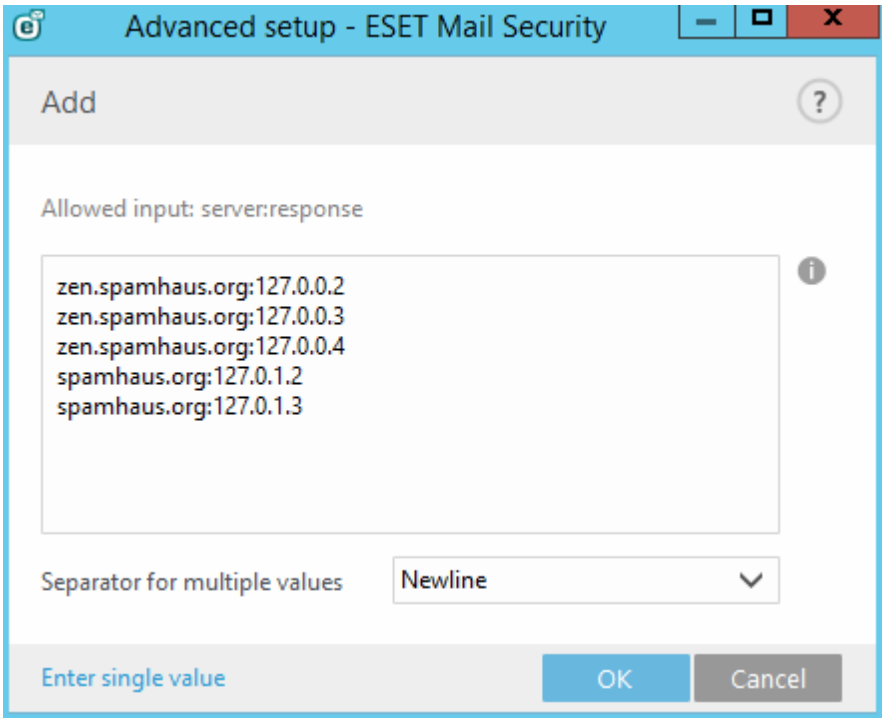
Verify sender's address against end-user blacklist. - Email messages that are not sent from mail servers (computers that are not listed as mail servers) are verified to make sure the sender is not on the blacklist. This option is enabled by default. You can disable it if required, but messages not sent from mail servers will not be checked against the blacklist.

Additional RBL servers - Is a list of Realtime Blackhole List (RBL) servers which are queried when analyzing messages.

NOTE: When adding Additional RBL servers, enter the server's domain name (e.g. `spamhaus.org`). It will work with any return codes that are supported by the server. For example:

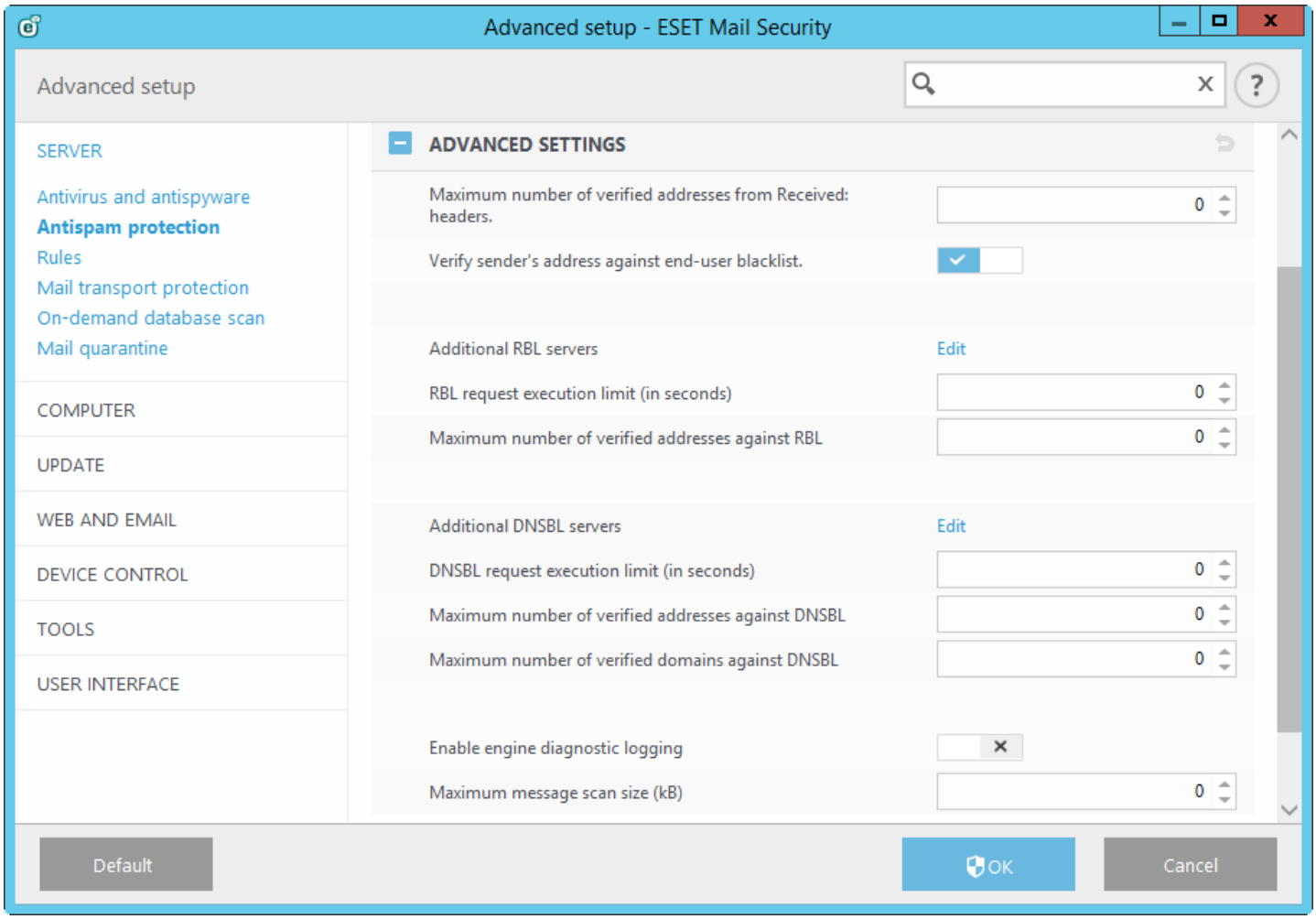


Alternatively, you can specify a server name with a return code in a form of `server:response` (e.g. `zen.spamhaus.org:127.0.0.4`). In this case we recommend you to add each server name and return code separately, so that you'll have a complete list. Click **Enter multiple values** in the Add pop-up window to specify all server names with their return codes. Entries should look like this example, your actual RBL server host names and return codes may vary:



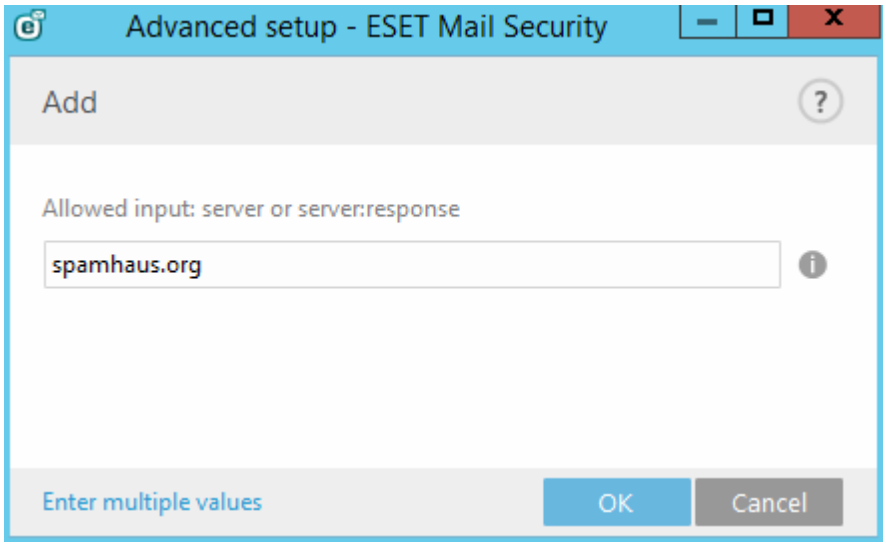
RBL request execution limit (in seconds) - This option allows you to set a maximum time for RBL queries. RBL responses are only used from those RBL servers which respond in time. If the value is set to "0" no timeout is enforced.

Maximum number of verified addresses against RBL - This option allows you to limit how many IP addresses are queried against the RBL server. Note that the total number of RBL queries will be the number of IP addresses in the Received: headers (up to a maximum of RBL maxcheck IP addresses) multiplied by the number of RBL servers specified in RBL list. If the value is set to "0" an unlimited number of received headers are checked. Note that IPs on the ignored IP list do not count towards the RBL IP addresses limit.



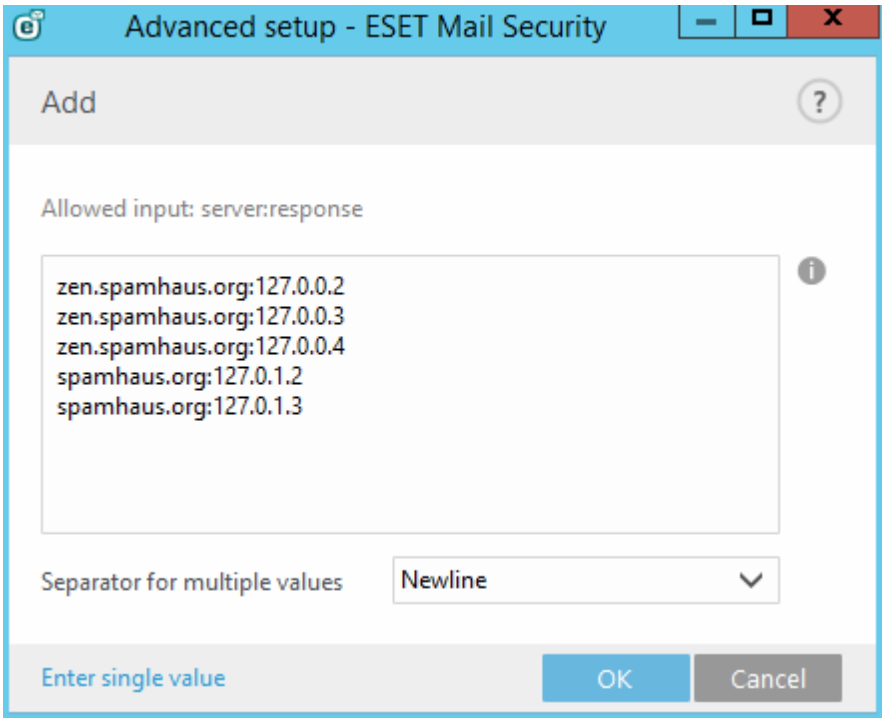
Additional DNSBL servers - Is a list of DNS Blocklist (DNSBL) servers which are queried with domains and IP addresses extracted from the message body.

NOTE: When adding Additional DNSBL servers, enter the server's domain name (e.g. `spamhaus.org`). It will work with any return codes that are supported by the server. For example:



Alternatively, you can specify a server name with a return code in a form of `server:response` (e.g. `zen.spamhaus.org:127.0.0.4`). In this case we recommend you to add each server name and return code separately,

so that you'll have a complete list. Click **Enter multiple values** in the Add pop-up window to specify all server names with their return codes. Entries should look like this example, your actual DNSBL server host names and return codes may vary:



DNSBL request execution limit (in seconds) - Allows you to set a maximum timeout for all DNSBL queries to complete.

Maximum number of verified addresses against DNSBL - Allows you to limit how many IP addresses are queried against the DNS Blocklist server.

Maximum number of verified domains against DNSBL - Allows you to limit how many domains are queried against the DNS Blocklist server.

Enable engine diagnostic logging - Writes detailed information about the Antispam engine into the log file for diagnostic purposes. Antispam engine doesn't use the **Events** log (`warnlog.dat` file) and therefore cannot be viewed in Log files viewer. It writes records directly into a dedicated text file (for example `C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log`) so that all Antispam engine diagnostic data are kept in one place. This way, performance of ESET Mail Security is not compromised in a case of a huge email traffic.

Maximum message scan size (kB) - Limits Antispam scan for messages larger than the specified value. These messages will not be scanned by the Antispam engine. Behavior:

If Maximum message scan size is set to: 0 = unlimited scan
If Maximum message size is set to: 1 - 12288 = 12288
If Maximum message size is set to: more than 12288 = set value
Recommended minimum value is 100kB.

5.1.4.3 Greylisting settings

The **Enable Greylisting** function activates a feature that protects users from spam using the following technique: The transport agent will send a “temporarily reject” SMTP return value (default is 451/4.7.1) for any received email that is not from a recognized sender. A legitimate server will try to resend the message after a delay. Spam servers will typically not attempt to resend the message, as they usually go through thousands of email addresses and do not waste time resending. Greylisting is an additional layer of antispam protection, and does not have any effect on the spam evaluation capabilities of the antispam module.

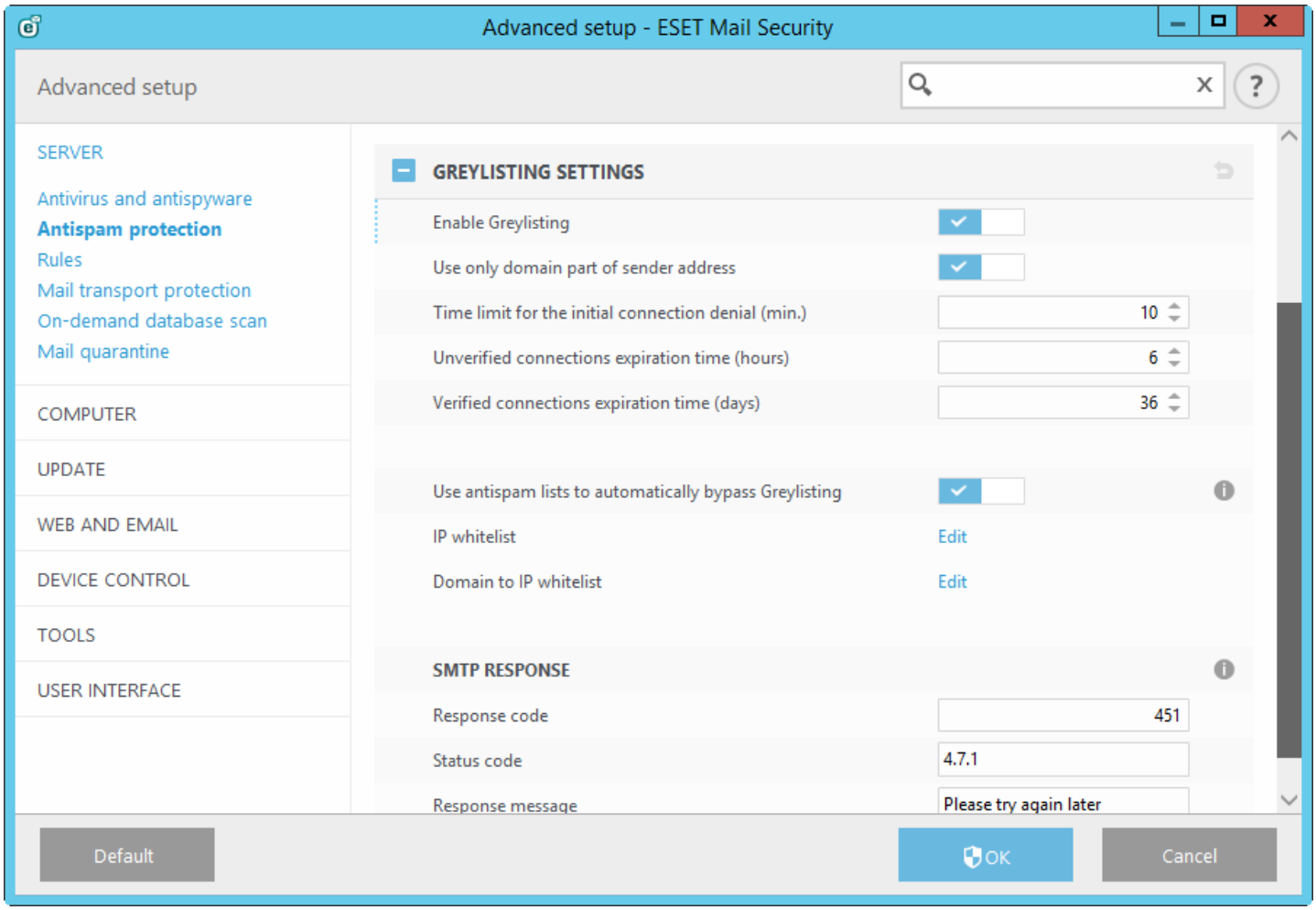
When evaluating the message source, the Greylisting method takes into account the **Approved IP list**, the **Ignored IP list**, **Safe Senders** and the **Allow IP lists** on the Exchange server as well as AntispamBypass settings for the recipient mailbox. Emails from these IP addresses/senders lists or emails delivered to a mailbox that has the AntispamBypass option enabled will be bypassed by the Greylisting detection method.**Use only domain part of sender address** -

ignores recipient's name in the email address; only domain is taken into account.

Time limit for the initial connection denial (min.) - when a message is delivered for the first time and temporarily refused, this parameter defines the time period during which the message will always be refused (measured from the first refusal). After the defined time period has elapsed, the message will be successfully received. The minimum value you can enter is 1 minute.

Unverified connections expiration time (hours) – this parameter defines the minimum time interval for which the triplet data will be stored. A valid server must resend a desired message before this period expires. This value must be greater than the value of **Time limit for the initial connection denial**.

Verified connections expiration time (days) – the minimum number of days for which the triplet information is stored, during which emails from a particular sender will be received without any delay. This value must be greater than the value of **Unverified connections expiration time**.



Use antispam lists to automatically bypass Greylisting - when enabled, Approved and Ignored IP list will be used together with IP whitelists to automatically bypass Greylisting.

IP whitelist - In this section, you can add IP address, IP address with mask, IP range. You can modify the list by clicking **Add**, **Edit** or **Remove**. Alternatively, you can **Import** or **Export** files. Use the browse button **...** to select a location on your computer to open or save the configuration file.

Domain to IP whitelist - This option allows you to specify domains (e.g. *domainname.local*). To manage the list, use **Add** or **Remove**.

SMTP response (for temporarily denied connections) - you can specify a **Response code**, **Status code** and **Response message**, which define the SMTP temporary denial response sent to the SMTP server if a message is refused.

Example of a SMTP reject response message:

Response code	Status code	Response message
451	4.7.1	Requested action aborted: local error in processing

WARNING: Incorrect syntax in SMTP response codes may lead to the malfunction of Greylisting protection. As a result, spam messages may be delivered to clients or messages may not be delivered at all.

NOTE: You can also use system variables when defining the SMTP reject response.

5.1.5 Rules

The **Rules** allow administrators to manually define email filtering conditions and actions to take with filtered emails.

There are three separate sets of rules. Rules available in your system depend on which Microsoft Exchange Server version is installed on the server with ESET Mail Security:

- Mailbox database protection - This type of protection is only available for Microsoft Exchange Server 2010, 2007 and 2003 operating in the Mailbox Server (Microsoft Exchange 2010 and 2007) or Back-End server (Microsoft Exchange 2003) role. This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it includes the Mailbox or Back-End role).
- Mail transport protection - This protection is provided by the transport agent and is only available for Microsoft Exchange Server 2007 or newer operating in the Edge Transport Server or Hub Transport Server role. This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles).
- On-demand database scan - allows you to execute or schedule an Exchange mailbox database scan. This feature is only available for Microsoft Exchange Server 2007 or newer operating in the Mailbox server or Hub Transport role. This also applies to a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles). See Exchange Server 2013 roles for some specifics regarding roles in Exchange 2013.

5.1.5.1 Rules list

The **Rules** list window displays existing rules. Rules are classified into three levels and are evaluated in this order:

- **Filtering rules (1)**
- **Attachment processing rules (2)**
- **Result processing rules (3)**

Rules with the same level are evaluated in the same order as they are displayed in the Rules window. You can only change the rule order for rules of the same level. For example, when you have multiple filtering rules, you can change the order they are applied in. You cannot change their order by putting Attachment processing rules before Filtering rules, the Up/Down buttons will not be available. In other words, you cannot mix rules of different Levels.

The Hits column displays the number of times the rule was successfully applied. Deselecting a check box (to the left of each rule name) deactivates the corresponding rule until you select the check box again.

- **Add...** - adds a new rule
- **Edit...** - modifies an existing rule
- **Remove** - removes selected rule
- **Move up** - moves the selected rule up in the list
- **Move down** - moves the selected rule down in the list
- **Reset** - resets the counter for the selected rule (the Hits column)

NOTE: If a new rule is added or an existing rule has been modified, message rescan will automatically start using the new/modified rules.

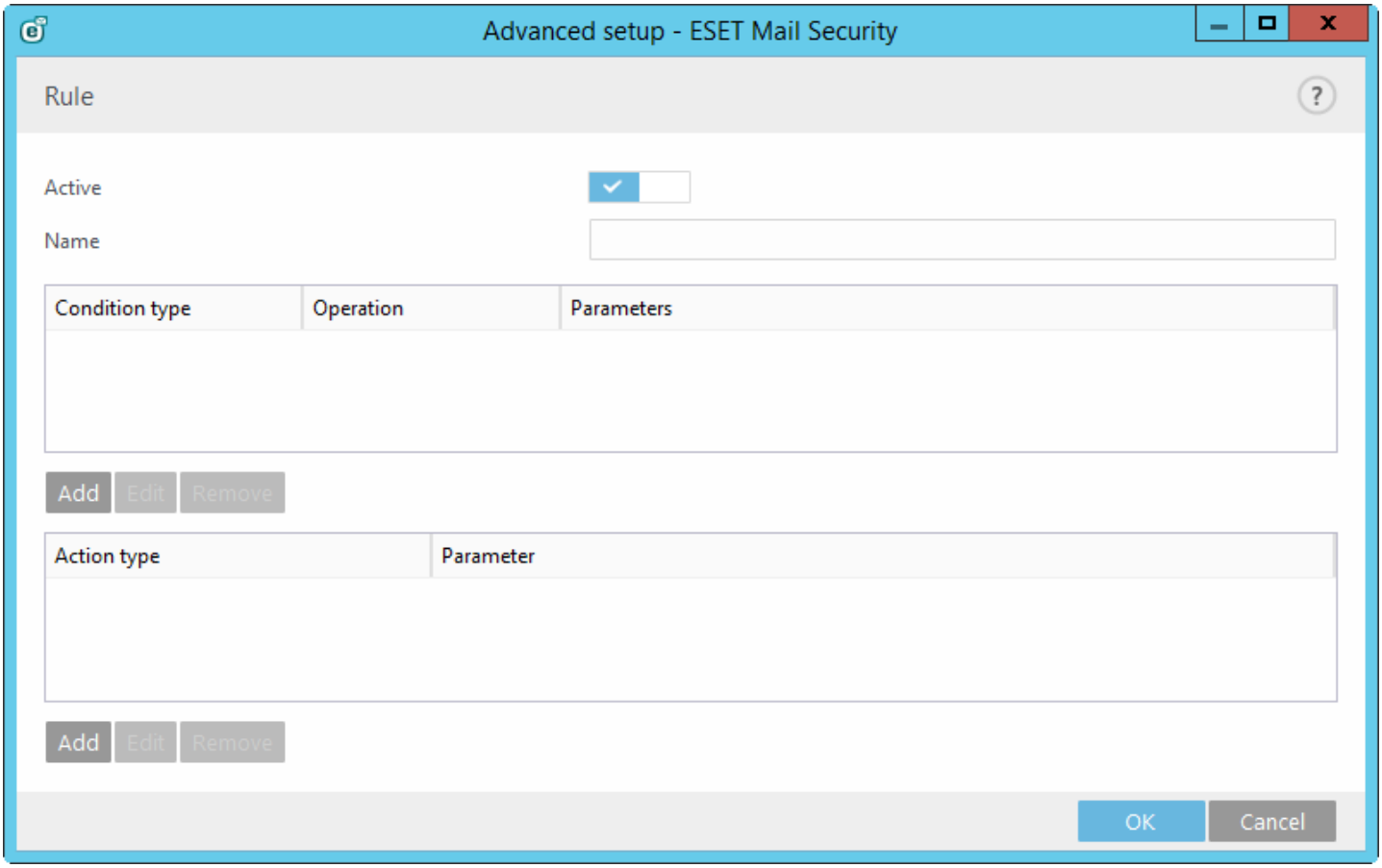
Rules are checked against a message when it is processed by the transport agent (TA) or VSAPI. When both the TA and VSAPI are enabled and the message matches the rule conditions, the rule counter may increase by 2 or more. This is because the VSAPI accesses the body and attachment of a message separately, so rules are applied to each part individually. Rules are also applied during background scanning (for example, when ESET Mail Security performs a mailbox scan following the download of a new virus signature database), which can increase the rule counter.

5.1.5.1.1 Rule wizard

You can define **Conditions** and **Actions** using the **Rule** wizard. Define Condition(s) first, then Action(s). Click **Add** and a Rule condition window will appear where you can select condition type, operation and value. From here you can add a Rule action. Once conditions and actions are defined, type a **Name** for the rule (something that you'll recognize the rule by), this name will be displayed in the Rules list. If you want to prepare rules but plan to use them later, you can click the switch next to **Active** to deactivate the rule. To activate the rule, select the check box next to the rule you want to activate from the Rules list.

NOTE: **Name** is a mandatory field, if it is highlighted in red, type rule name in the text box and click **OK** button to create the rule. Red highlight does not disappear even though you've entered rule name, it disappears only after you've clicked **OK**.

Some **Conditions** and **Actions** differ for rules specific to **Mail transport protection**, **Mailbox database protection** and **On-demand database scan**. This is because each of these protection types use a little different approach when processing messages, especially **Mail transport protection**.



NOTE: If you configure Action type **Log to events** for Mailbox database protection with parameter %IPAddress%, the **Event** column in the Log files will be empty for this particular event. This is because there is no IP address on Mailbox database protection level. Some options are not available on all protection levels:

IP address - ignored by **On-demand database scan** and **Mailbox database protection**
Mailbox - ignored by **Mail transport protection**

5.1.5.1.1.1 Rule condition

This wizard lets you add conditions for a rule. Select **Type** > **Operation** from the drop-down list (the list of operations changes depending on what rule type you've chosen) and select **Parameter**. Parameter fields will change depending on rule type and operation.

For example, choose **Attachment size** > **is greater than** and under **Parameter** specify 10 MB. Using these settings, any message that contains an attachment larger than 10 MB will be processed using the rule action you have specified. For this reason you should specify the action that is taken when a given rule is triggered if you have not done so when setting parameters for that rule.

NOTE: It is possible to add multiple conditions for one rule.

The following Conditions are available for **Mail transport protection**, **Mailbox database protection** and **On-demand database scan** (some of the options might not display depending on your previously selected conditions):

Conditions name	Mail transport protection	Mailbox database protection	On-demand database scan	Descriptions
Subject	x	x	x	Applies to messages which contain or do not contain a specific string (or a regular expression) in the subject.
Sender	x	x	x	Applies to messages sent by a specific sender.
Sender's IP address	x			Applies to messages sent from a specific IP address.
Sender's domain	x	x	x	Applies to messages from a sender with a specific domain in their email addresses.
Recipient	x	x	x	Applies to messages sent to a specific recipient.
Recipient's organizational units	x			Applies to messages sent to a recipient of a specific organizational unit.
Attachment name	x	x	x	Applies to messages containing attachments with a specific name.
Attachment size	x	x	x	Applies to messages with an attachment that does not meet a specified size, is within a specified size range, or exceeds a specified size.
Attachment type	x	x	x	Applies to messages with a specific file type attached. File types are categorized in groups for easy selection, you can select multiple file types or whole categories.
Message size	x			Applies to messages with attachments that do not meet a specified size, are within a specified size range or exceed a specified size.
Mailbox		x		Applies to messages located in a specific mailbox.
Message headers	x	x		Applies to messages with specific data present in the message header.
Antispam scan result	x			Applies to messages flagged or not flagged as Ham or Spam.
Antivirus scan result	x	x	x	Applies to messages flagged as malicious or not malicious.
Internal message	x			Applies depending on whether a message is internal or not internal.

Received time	x	x	x	Applies to messages received before or after a specific date, or during a specific date range.
Contains password protected archive	x	x	x	Applies to messages with archive attachments that are protected by a password.
Contains damaged archive	x	x	x	Applies to messages with archive attachments that are damaged (most likely impossible to open).

5.1.5.1.1.2 Rule action

You can add actions that will be taken with messages and/or attachments that match rule conditions.

NOTE: It is possible to add multiple conditions for one rule.

The list of available **Actions** for **Mail transport protection**, **Mailbox database protection** and **On-demand database scan** (some of the options might not show up depending on your selected conditions):

Actions name	Mail transport protection	Mailbox database protection	On-demand database scan	Descriptions
Quarantine message	x			The message will not be delivered to the recipient and will be moved to the mail quarantine.
Delete attachment	x	x	x	Deletes a message attachment the message will be delivered to the recipient without the attachment.
Reject message	x			The message will not be delivered and a NDR (Non-Delivery Report) will be sent to the sender.
Drop message silently	x			Deletes a message without sending a NDR.
Set SCL value	x			Changes or sets a specific SCL value.
Send email notification	x	x	x	Sends email notifications to a recipient specified in Email notifications. You need to enable Send event notification by email feature. You can then customize the format of event messages (use the tooltip for suggestions) while creating the rule. Also, you can select verbosity for event messages, however this depends on the minimum verbosity setting in Email notifications section.
Skip Antispam scan	x			Message will be scanned by the Antispam engine.
Skip Antivirus scan	x	x	x	Message will be scanned by the antivirus engine.
Evaluate other rules	x	x	x	Allows the evaluation of other rules, enabling the user to define multiple sets of conditions and multiple actions to take given the conditions.
Log to events	x	x	x	Writes information about the applied rule to the program log and define the format of event messages (use the tooltip for suggestions).
Add header field	x			Adds a custom string to a message header.
Replace attachment with action information		x	x	Removes an attachment and adds information about action taken with the attachment to the email body.
Quarantine		x	x	Puts email attachment into file quarantine, email will be

attachment				delivered to the recipient with the attachment truncated to zero length.
Delete message			**x**	Delete an infected message.
Move message to trash			**x**	Puts an email message into the trash folder on the email client's side.

5.1.6 Mail transport protection

The following operating systems have **Mail transport protection** available in **Advanced settings** > **Server**:

- Microsoft Exchange Server 2007 (Edge Transport Server or Hub Transport Server)
- Microsoft Exchange Server 2007 (single server installation with multiple roles)
- Microsoft Exchange Server 2010 (Edge Transport Server or Hub Transport Server)
- Microsoft Exchange Server 2010 (single server installation with multiple roles)
- Microsoft Exchange Server 2013 (Edge Transport server role)
- Microsoft Exchange Server 2013 (single server installation with multiple roles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

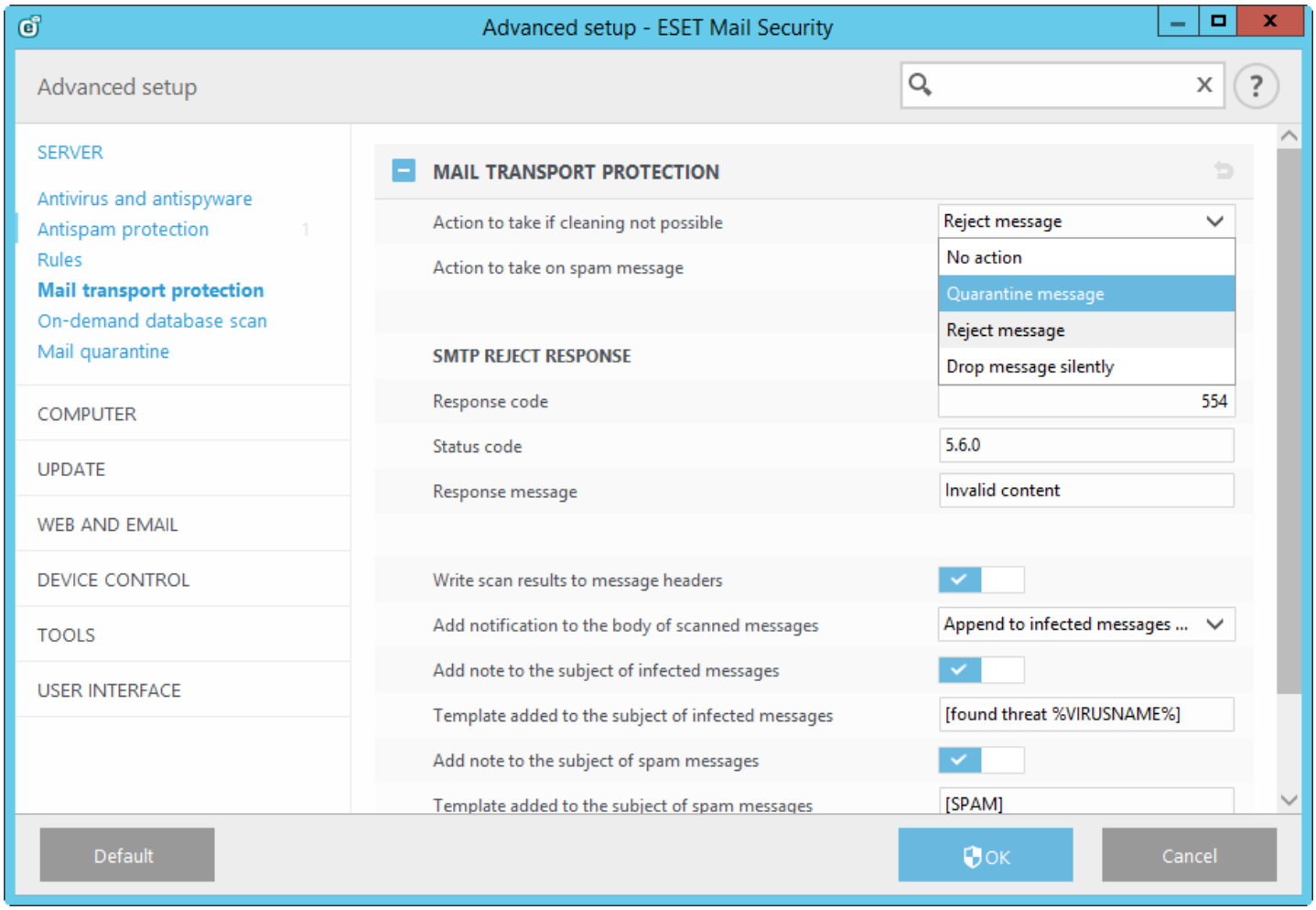
Antivirus action on the transport layer can be set under **Actions to take if cleaning not possible**:

- **No action -** retain infected messages that cannot be cleaned
- **Quarantine message -** send infected messages to the quarantine mailbox
- **Reject message -** reject an infected message
- **Drop message silently** - deletes messages without sending NDR (Non-Delivery Report)

NOTE: If you select **No action** and at the same time have **Cleaning level** set to **No cleaning** in ThreatSense parameters of Antivirus and antispyware, then the protection status will change to yellow. This is because it is a security risk and we do not recommend you to use this combination. Change one or the other setting in order to achieve a good level of protection.

Antispam action on transport layer can be set under **Action to take on spam messages**:

- **No action** - keep the message even if it is marked as spam
- **Quarantine message** - send messages marked as spam to the quarantine mailbox
- **Reject message -** reject messages marked as spam
- **Drop message silently** - delete messages without sending NDR (Non-Delivery Report)



SMTP Reject Response - you can specify a **Response code**, **Status code** and **Response message** which define the SMTP temporary denial response sent to the SMTP server if a message is refused. You can enter a response message in the following format:

Response code	Status code	Response message
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted:local error in processing
550	5.5.0	Requested action not taken:mailbox unavailable
554	5.6.0	Invalid content

NOTE: You can also use system variables when configuring SMTP Reject Responses.

Write scan results to message headers - when enabled, a scan results are written into message headers. These message headers start with `X_ESET` making them easy to recognize (for example `X_EsetResult` or `X_ESET_Antispam`).

Add notification to the body of scanned messages offers three options:

- Do not append to messages
- Append to infected messages only
- Append to all scanned messages (doesn't apply to internal messages)

Add note to the subject of infected messages - when enabled, ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of infected messages** text field (predefined default text is `[found threat %VIRUSNAME%]`). This modification can be used to automate filtering of infected messages by filtering emails with a specific subject, for example using rules or alternatively on a client side

(if supported by the email client) to put such email messages into a separate folder.

Add note to the subject of spam messages - when enabled, ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of spam messages** text field (predefined default text it `[SPAM]`). This modification can be used to automate spam filtering by filtering emails with a specific subject, for example using rules or alternatively on a client side (if supported by the email client) to put such email messages into a separate folder.

NOTE: You can also use system variables when editing text which will be added to the subject.

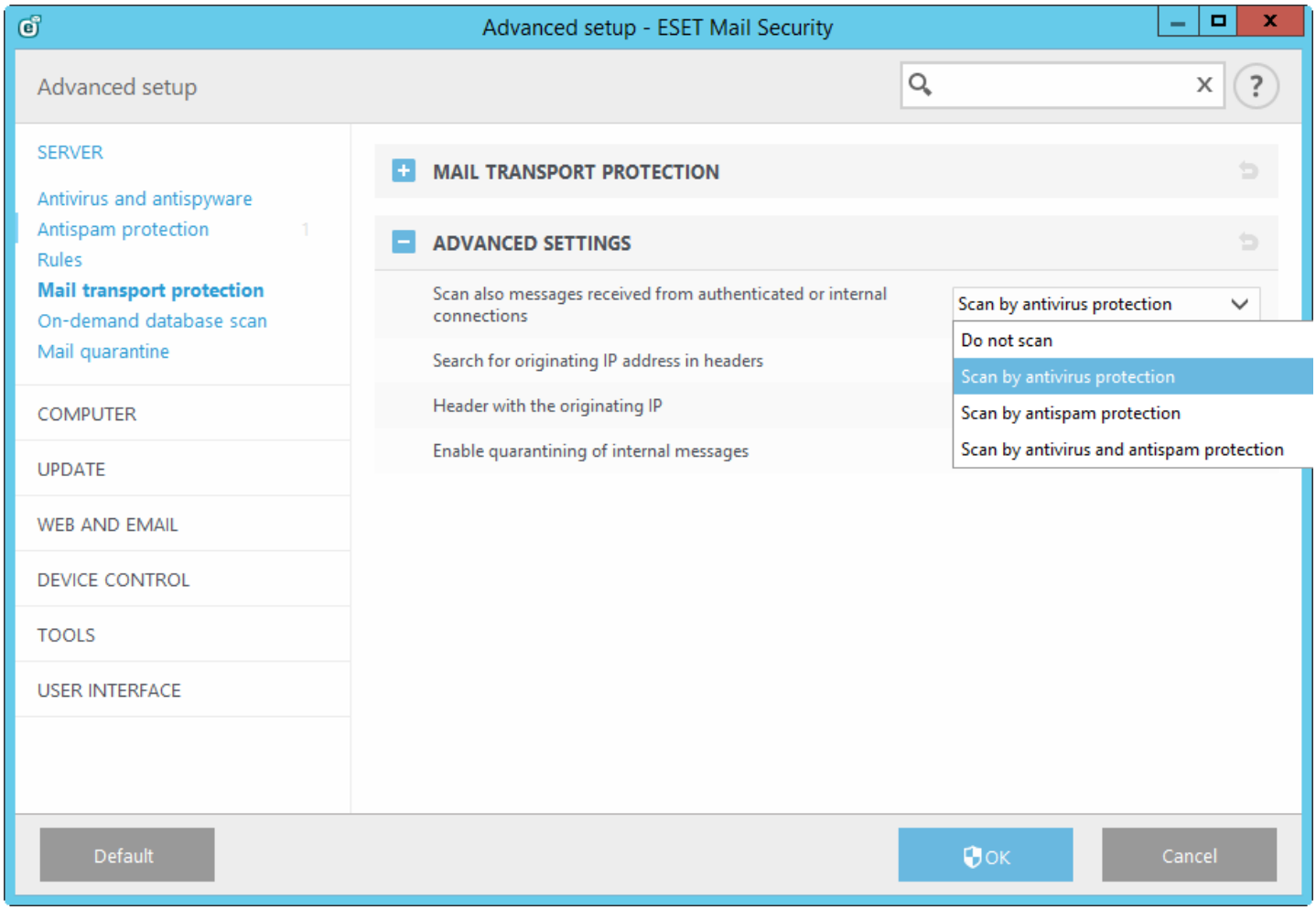
5.1.6.1 Advanced settings

In this section you can change advanced settings applied for the transport agent:

- **Scan also messages received from authenticated or internal connections** - you can choose what type of scan should be performed on messages received from authenticated sources or local servers. Scanning of such messages is recommended as it increases protection, but necessary if you are using built-in Microsoft SBS POP3 Connector to fetch email messages from external POP3 servers or mail services (for example **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem**, etc.). For more information see POP3 Connector and antispam.

NOTE: Internal messages from Outlook inside the organization are being sent in TNEF format (Transport Neutral Encapsulation Format). TNEF format is not supported by antispam. Therfore, internal TNEF formated emails will not be scanned for SPAM even though you have selected **Scan by antispam protection** or **Scan by antivirus and antispam protection**.

- **Search for originating IP address in headers** - if enabled, ESET Mail Security looks for originating IP address in message headers so that different protection modules (Antispam and others) can use it. In case your Exchange Organization is separated from the internet by a Proxy, Gateway or Edge Transport Server, email massages appear to arrive from single IP address (usually an internal one). It is common that on the outside server (for example Edge Transport in DMZ) where senders IP address is known, this IP address is written into the message headers of email message that is being received. Value specified in **Header with the originating IP** field below is the header that ESET Mail Security looks for in message headers.
- **Header with the originating IP** - is the header that ESET Mail Security looks for in message headers. Default is **X-Originating-IP**, but if you are using third party or custom tools that use different header, change it to an appropriate one.
- **Enable quarantining of internal messages** - when enabled, internal messages will be quarantined. There is usually no need to quarantine internal messages, however, if you require such quarantining, you can enable it.



5.1.7 Mailbox database protection

The following systems have **Mailbox database protection** available under **Advanced settings** > **Server**:

- Microsoft Exchange Server 2003 (Back-End server role)
- Microsoft Exchange Server 2003 (single server installation with multiple roles)
- Microsoft Exchange Server 2007 (Mailbox Server role)
- Microsoft Exchange Server 2007 (single server installation with multiple roles)
- Microsoft Exchange Server 2010 (Mailbox Server role)
- Microsoft Exchange Server 2010 (single server installation with multiple roles)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTE: Mailbox database protection is not available for Microsoft Exchange Server 2013.

If you deselect **Enable antivirus and antispyware protection VSAPI 2.6**, the ESET Mail Security plug-in for Exchange server will not be unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses. The messages however, will still be scanned for spam and the rules will be applied.

If **Proactive scanning** is enabled, new inbound messages will be scanned in the same order they are received. If this option is enabled and a user opens a message that has not been scanned yet, this message will be scanned before other messages in the queue.

Background scanning allows scanning of all messages to run in the background (scanning runs on the mailbox and public folders store, for example the Exchange database). Microsoft Exchange Server decides whether a background scan will run or not based on various factors such as the current system load, number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client. You can choose to **Scan only messages with attachments** and filter based on time received using the following **Scan level** options:

- **All messages**
- **Messages received within last year**
- **Messages received within last 6 months**
- **Messages received within last 3 months**
- **Messages received within last months**
- **Messages received within last week**

Since background scanning can affect system load (scanning is performed after each virus signature database update), we recommend that you schedule scans to run during non-work hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and you can modify its parameters, delete it or temporarily deactivate the task.

Enabling the **Scan RTF message bodies** option activates scanning of RTF message bodies. RTF message bodies may contain macro viruses.

NOTE: Plain text email bodies are not scanned by VSAPI.

NOTE: Public folders are treated the same way as mailboxes. This means that public folders are scanned as well.

5.1.8 On-demand database scan

List of systems that have **On-demand database scan** available:

- Microsoft Exchange Server 2007 (Mailbox server or Hub Transport Server)
- Microsoft Exchange Server 2007 (single server installation with multiple roles)
- Microsoft Exchange Server 2010 (Mailbox server or Hub Transport Server)
- Microsoft Exchange Server 2010 (single server installation with multiple roles)
- Microsoft Exchange Server 2013 (Mailbox server server role)
- Microsoft Exchange Server 2013 (single server installation with multiple roles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTE: If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Mailbox database protection and On-demand database scan. However, only one protection type out of these two can be active at a time. If you decide to use On-demand database scan you'll need to disable integration of Mailbox database protection in Advanced setup under Server. Otherwise On-demand database scan will not be available.

On-demand database scan settings:

Host address - Name or IP address of server running EWS (Exchange Web Services).
Username - Specify credentials of a user that has appropriate access to EWS (Exchange Web Services).
User password - Click **Set** next to **User password** and type password for this user account.

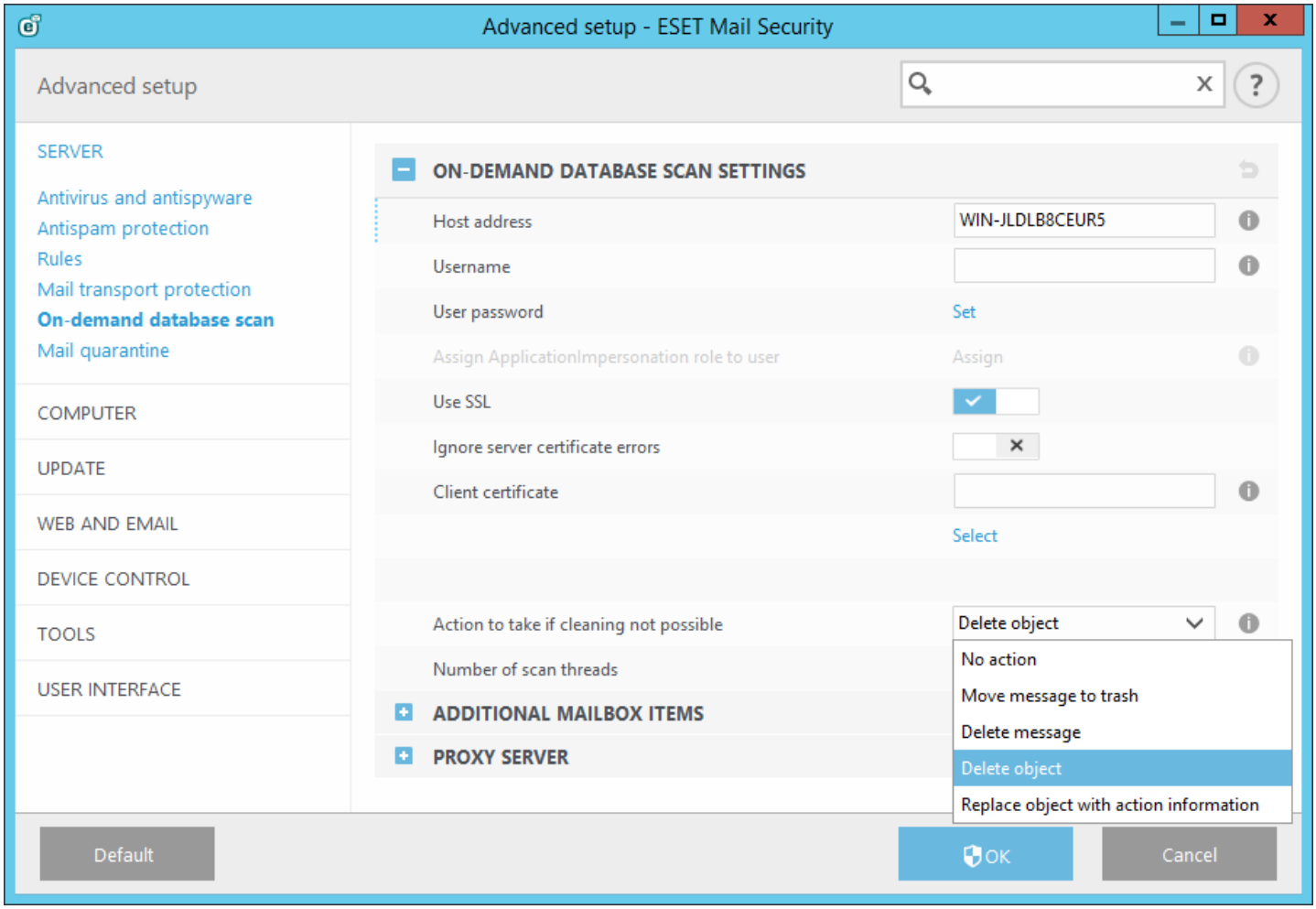
Assign ApplicationImpersonation role to user - If this option is grayed out, you need to specify **Username** first. Click **Assign** to automatically assign ApplicationImpersonation role to selected user. Alternatively, you can assign ApplicationImpersonation role manually to a user account. For more information see Database scan account details.

Use SSL - needs to be enabled if EWS (Exchange Web Services) is set to **Require SSL** in IIS. If SSL is enabled, Exchange Server certificate must be imported on the system with ESET Mail Security (in case Exchange Server roles are on

different servers). Settings for the EWS can be found in IIS in *Sites/Default web site/EWS/SSL Settings*.

NOTE: Disable **Use SSL** only in case you have EWS configured in IIS not to Require SSL.

Client certificate - Needs to be set only when Exchange Web Services requires client certificate. **Select** allows you to select any of the certificates.



Action to take if cleaning not possible - this actions field allows you to **block** infected content.

No action - take no action on the infected content of the message.
Move message to trash - is not supported for Public folder items. You can use **Delete object** action will be applied instead.
Delete object - infected content of the message.
Delete message - delete the entire message including it's infected content.
Replace object with action information - removes an object and puts information about the action that was taken with this object.

5.1.8.1 Additional mailbox items

On-demand database scanner settings lets you enable or disable scanning of other mailbox item types:

- Scan calendar
- Scan tasks
- Scan contacts
- Scan journal

NOTE: If you experience performance issues, you can disable scanning of these items. Scans will take longer when these items are enabled.

5.1.8.2 Proxy server

In case you use a proxy server between your Exchange Server with CAS role and Exchange Server where ESET Mail Security is installed, specify parameters of your proxy server. This is required because ESET Mail Security connects to EWS (Exchange Web Services) API via HTTP/HTTPS. Otherwise On-demand database scan will not work.

Proxy server - enter IP address or name of the proxy server you use.

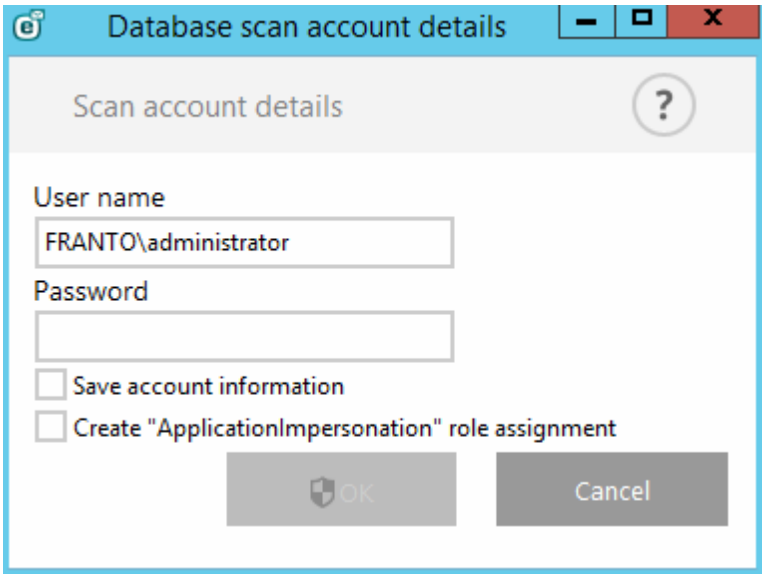
Port - enter port number of the proxy server.

Username, Password - enter credentials if your proxy server requires authentication.

5.1.8.3 Database scan account details

This dialog window displays if you have not specified a user name and password for **Database scan** in **Advanced setup**. Specify the credentials of the user who has access to EWS (Exchange Web Services) in this pop-up window and click **OK**. Alternatively, go to **Advanced setup** by pressing **F5** and navigate to **Server** > On-demand database scan. Type your **Username**, click **Set**, type a password for this user account and then click **OK**.

- You can select **Save account information** to save account settings, so that you won't have to enter account information every time you run an On-demand database scan.
- If a user account does not have appropriate access to EWS, you can select **Create "ApplicationImpersonation" role assignment** to assign this role to an account. Alternatively, you can assign ApplicationImpersonation role manually, see Note below for details.



IMPORTANT: Scan account must have **ApplicationImpersonation** rights assigned in order for the scan engine to scan user mailboxes within Exchange mailbox database(s). On Exchange Server 2010 or newer, we highly recommend you to configure Throttling Policy for the scan account in order to prevent too many operation requests by ESET Mail Security. Otherwise your Exchange Server might cause some of the operation requests to timeout.

NOTE: If you want to assign ApplicationImpersonation role to a user account manually, you can use following commands (replace `ESET-user` with an actual account name in your system):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation

Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

This might take a few moments to apply

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -EWSFastSearchTimeoutInSeco

Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2013

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

This might take a few moments to apply

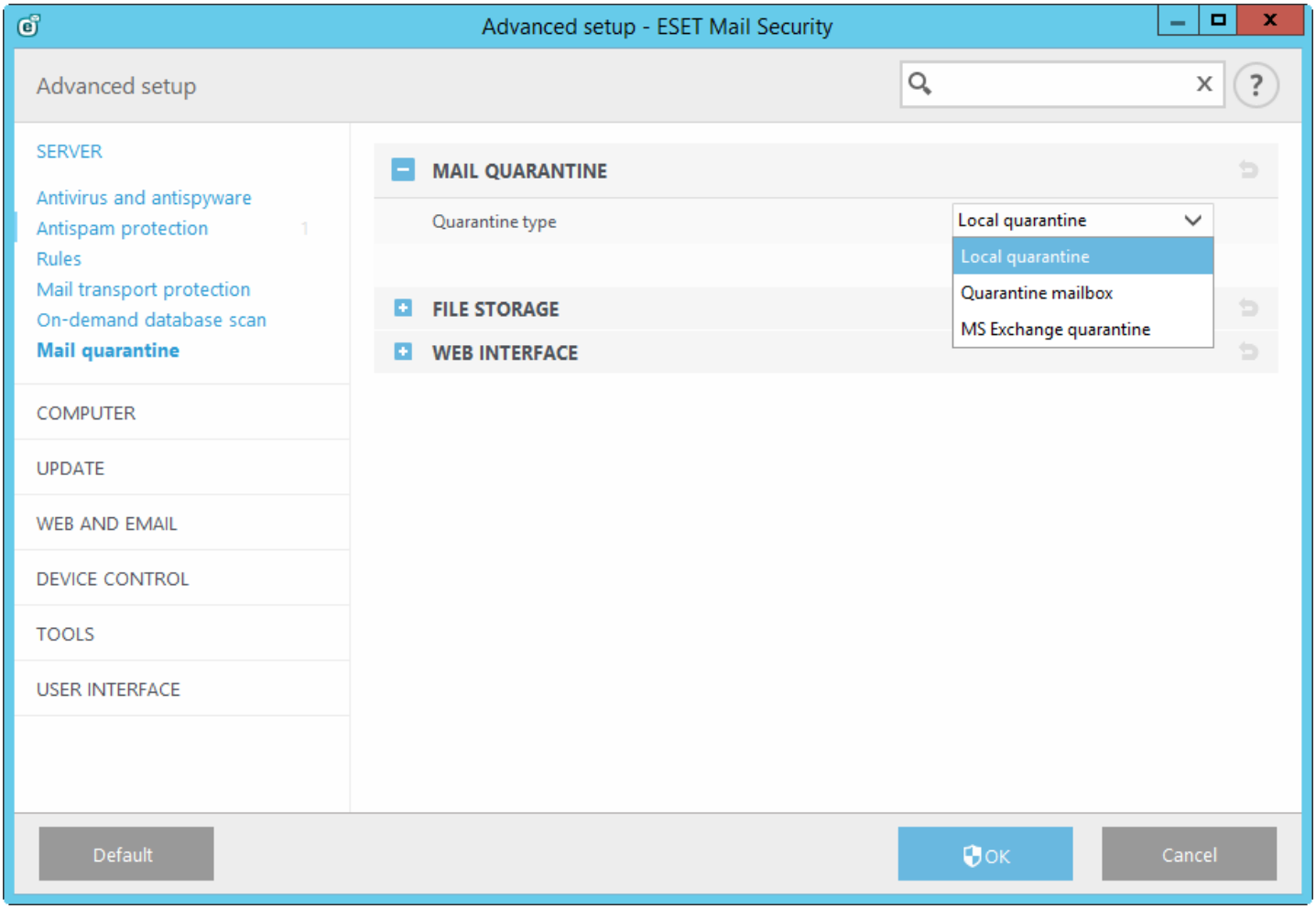
```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlim

Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-ThrottlingPolicy
```

5.1.9 Mail Quarantine

The Mail Quarantine manager is available for all three Quarantine types:

- Local quarantine
- Quarantine mailbox
- MS Exchange quarantine



You can see the contents of the Mail Quarantine in Mail Quarantine manager for all Quarantine types. Additionally, the local quarantine can also be viewed in the Mail Quarantine Web interface.

5.1.9.1 Local quarantine

The Local quarantine uses the local file system to store quarantined emails and a SQLite database as an index. Stored quarantined email files as well as database file are encrypted for security reasons. These files are located under `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (on Windows Server 2008 and 2012) or `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (on Windows Server 2003).

NOTE: If you want to have quarantined files stored on a different disk, other than the default `C:` drive, you need to change the **Data folder** to your preferred path during installation of ESET Mail Security.

Local quarantine features:

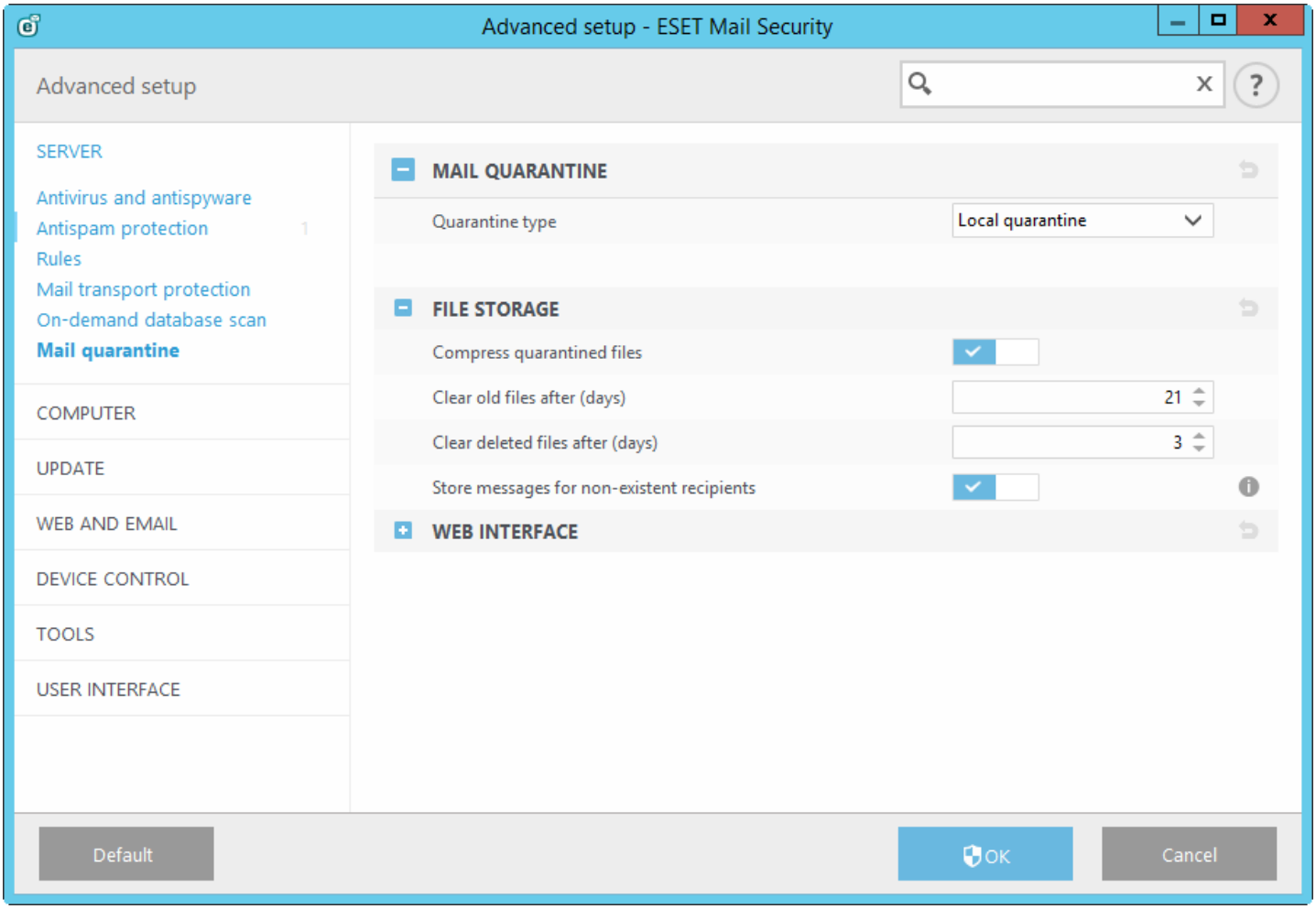
- SPAM and quarantined email messages will be stored in a local file system, which means that these will not be contained in Exchange mailbox database.
- Encryption and compression of locally stored quarantined email files.
- Mail Quarantine Web interface as an alternative to Mail quarantine manager.
- Quarantine reports can be sent to a specified email address using a scheduled task.
- Quarantined email files removed from the quarantine window (after 21 days by default), are still stored in a file system (until automatic deletion occurs after a specified number of days)
- Automatic deletion of old email files (after 3 days by default). For more information see File storage settings.
- You can restore removed quarantined email files using eShell (assuming that they've not been deleted from the file system yet).

NOTE: The downside of using Local quarantine is that if you run ESET Mail Security multiple servers with Hub Transport Server role, you need to manage each server's Local quarantine separately. The more the servers the more the quarantines to manage.

You can inspect quarantined email messages and decide to **delete** or **release** any of them. To view and manage locally quarantined email messages, you can use either Mail Quarantine manager from the main GUI or Mail Quarantine Web interface.

5.1.9.1.1 File storage

In this section you can change settings for file storage used by the local quarantine.



Compress quarantined files - compressed quarantined files take up less disk space, but if you decide not to have files compressed then use the switch to turn off compression.

Clear old files after (days) - when messages reach specified number of days, these are removed from the quarantine window. However, files will not be deleted from the disk for the amount of days specified in **Clear deleted files after (days)**. Since files are not deleted from the file system, it is possible to recover such files using eShell.

Clear deleted files after (days) - deletes files from the disk after specified number of days, no recovery is possible after these were deleted (unless you have file system backup solution in place).

Store messages for non-existent recipients - usually spam messages are sent to random recipients for a certain domain in an attempt to hit an existing one. Messages sent to users that do not exist in an Active Directory are stored in Local quarantine by default. However, you can turn this off and messages to non-existent recipients will not be stored, this way your Local quarantine will not be overflown by many spam messages of this type. This also saves disk space.

5.1.9.1.2 Web interface

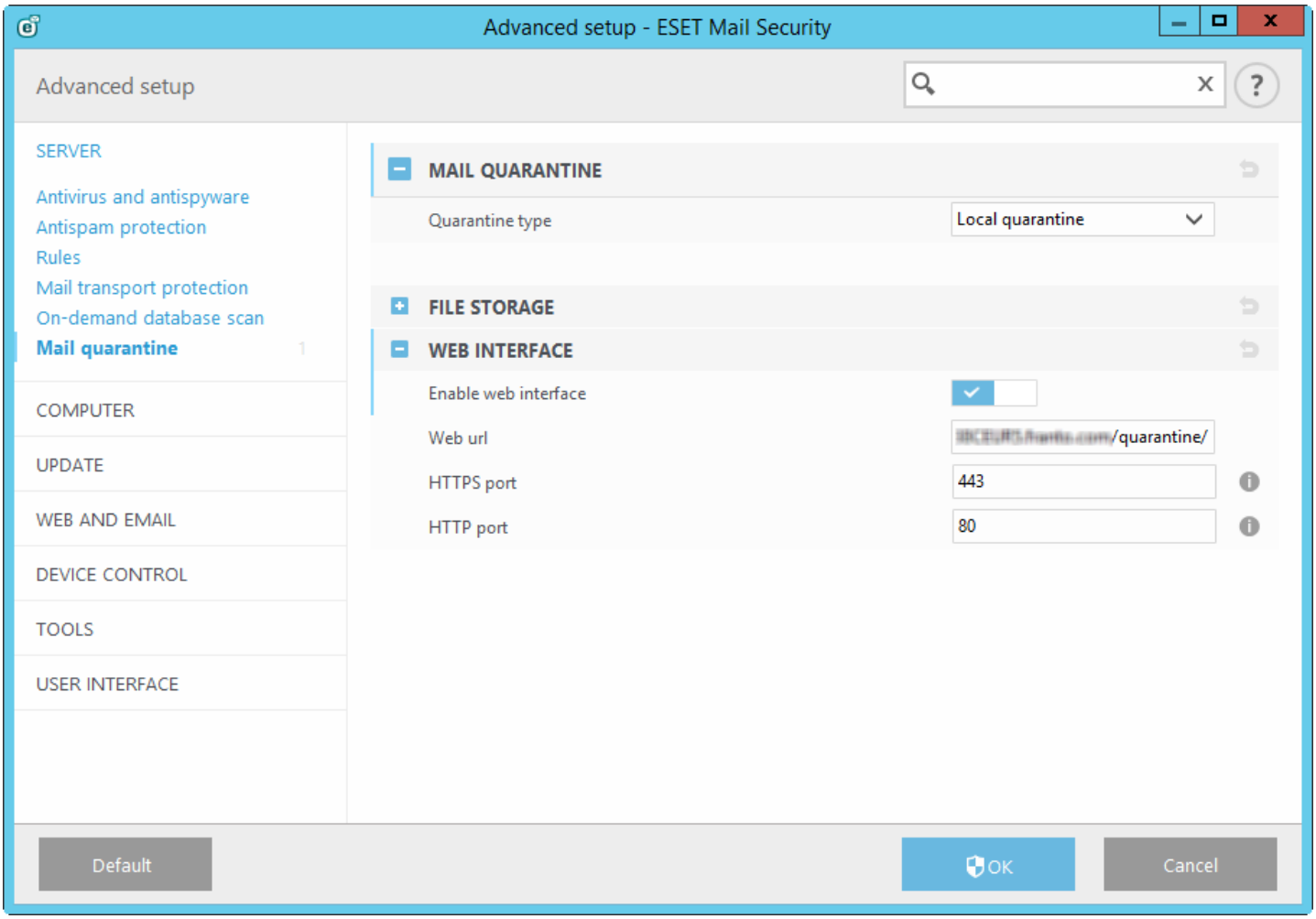
The Mail Quarantine Web interface is an alternative to Mail quarantine manager, however, it is only available for the Local quarantine.

NOTE: Mail Quarantine Web interface is not available on a server with Edge Transport Server role. It is because the Active Directory is not accessible for authentication.

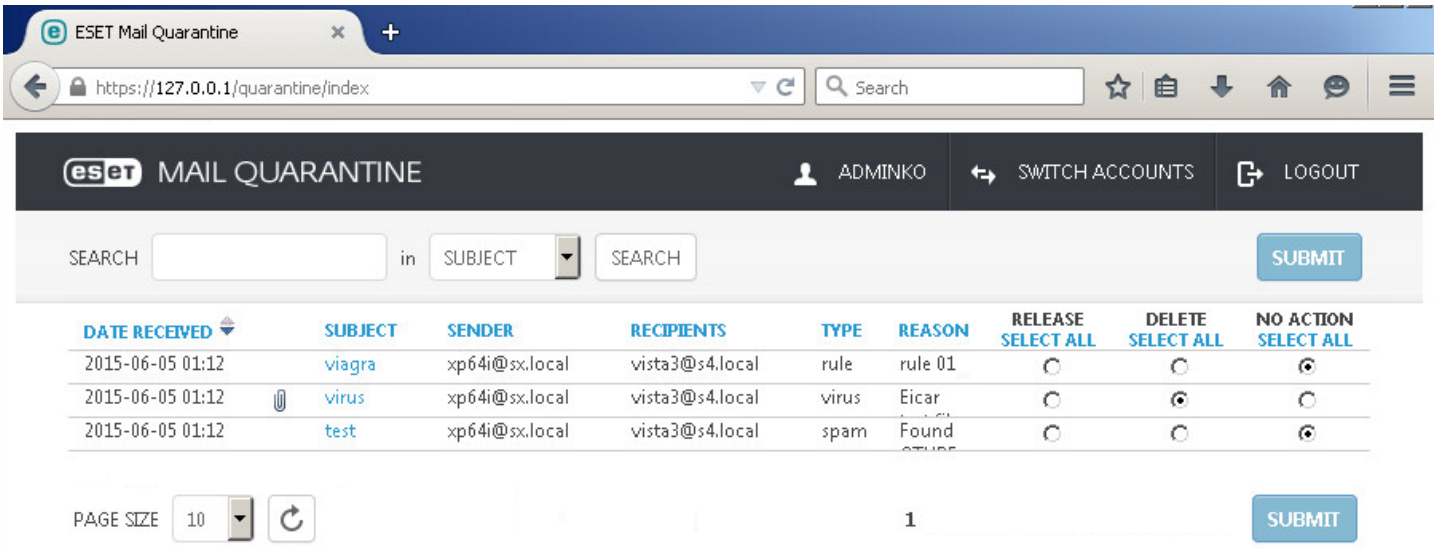
The Mail Quarantine Web interface allows you to view the state of the mail quarantine. It also lets you manage quarantined email objects. This web interface is accessible via links from quarantine reports or directly by entering a URL into a your web browser. To access the Mail Quarantine web interface, you must authenticate using domain credentials. Internet Explorer will authenticate automatically for a domain user; the web page certificate must be valid, Automatic logon must be enabled in IE, and you must add the Mail Quarantine web site to Local intranet sites.

The **Enable web interface** switch lets you disable or enable the web interface.

Web url - this is the URL on which the Web interface of Mail Quarantine will be available. By default, it is FQDN of the server with `/quarantine` (e.g. `mailserver.company.com/quarantine`).
HTTPS port - default port number is 443. You can change the port number if required.
HTTP port - default port number is 80. You can change the port number if required.

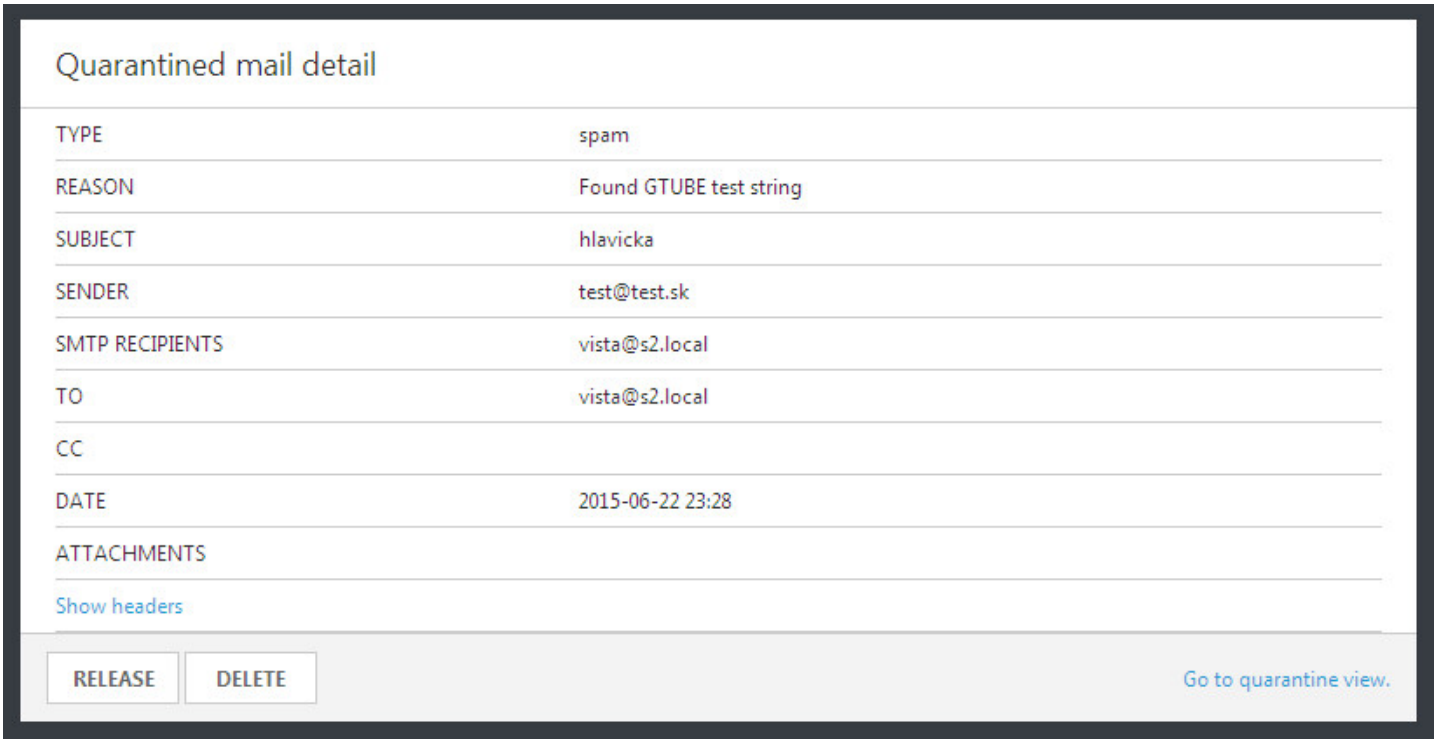


To access the Web interface of Mail Quarantine, open your web browser and use the URL specified in **Advanced setup** > **Server** > **Mail quiaratine** > **Web interface** > **Web url**.

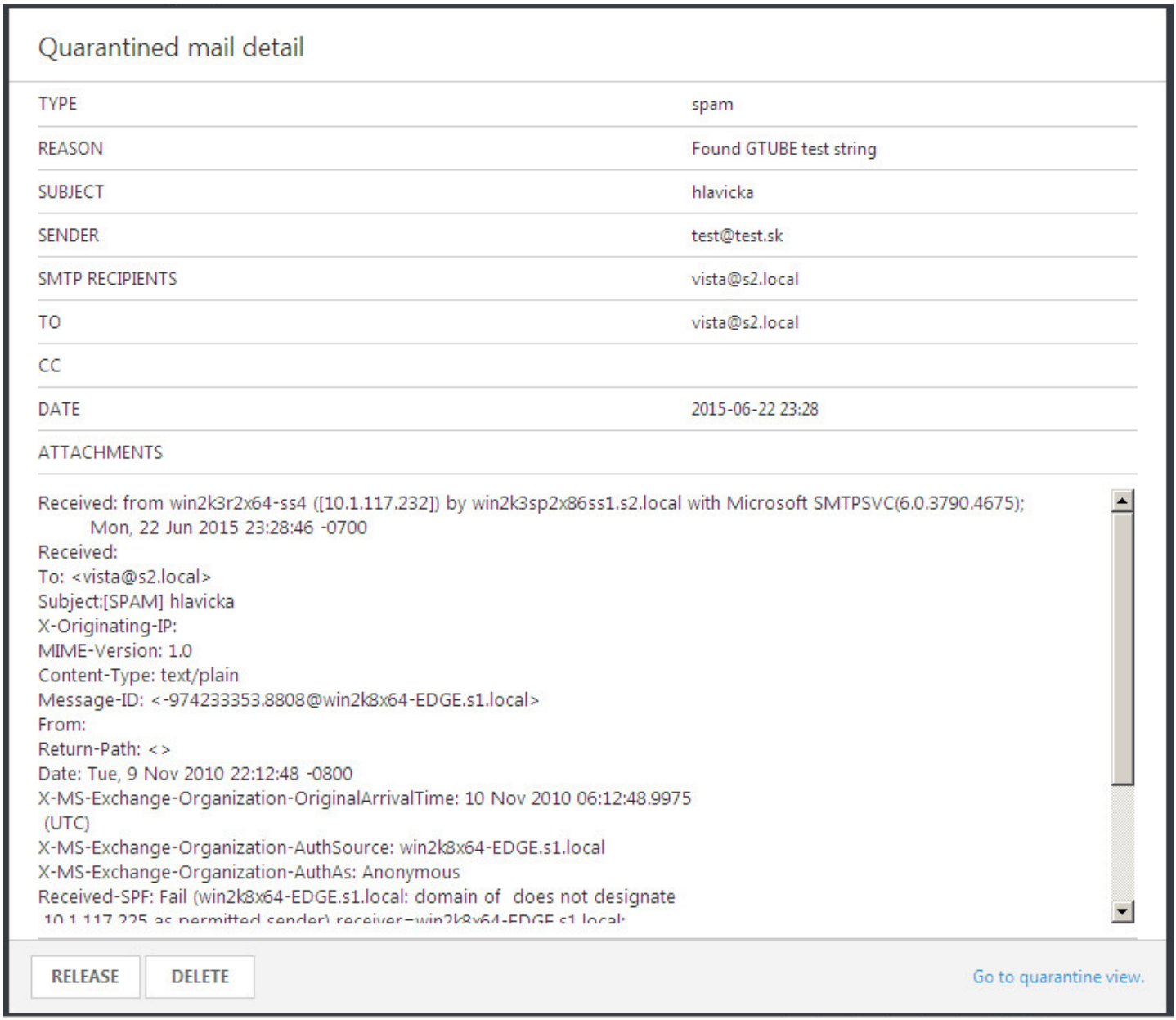


Release - releases email to its original recipient(s) using the Replay directory and deletes it from quarantine. Click **Submit** to confirm the action.
Delete - deletes item from quarantine. Click **Submit** to confirm the action.

When you click **Subject**, a pop-up window will open with details about the quarantined email such as **Type**, **Reason**, **Sender**, **Date**, **Attachments**, etc.



Click **Show headers** to review the header of the quarantined email.



If desired, click **Release** or **Delete** to take action with a quarantined email message.

NOTE: You must close your browser window to completely log out of the Mail Quarantine Web interface. Otherwise, click **Go to quarantine view** to return to the previous screen.

IMPORTANT: If you are having problems accessing the Mail Quarantine Web interface from your browser or are getting the error `HTTP Error 403.4 - Forbidden` or similar, check to see which Quarantine type is selected and make sure it is **Local quarantine** and that **Enable web interface** is enabled.

5.1.9.2 Quarantine mailbox and MS Exchange quarantine

If you decide not to use Local quarantine you have two options, either **Quarantine mailbox** or **MS Exchange quarantine**. Whichever option you choose, you need to create dedicated user with mailbox (for example main_quarantine@company.com) which will then be used to store quarantined email messages. This user and mailbox will also be used by Mail Quarantine manager to view and manage items in the quarantine. You'll need to specify account details of this user in Quarantine manager settings.

IMPORTANT: We do not recommend you to use Administrator user account as quarantine mailbox.

NOTE: **MS Exchange quarantine** is not available for Microsoft Exchange 2003, only **Local quarantine** and **Quarantine mailbox**.

- When you select **MS Exchange quarantine**, ESET Mail Security will use **Microsoft Exchange quarantine system** (this applies to Microsoft Exchange Server 2007 and newer). In this case, the Exchange's internal mechanism is used to store potentially infected messages and SPAM.

NOTE: By default, internal quarantine is not activated within Exchange. In order to activate it, you need to open Exchange Management Shell and type in following command (replace `name@domain.com` with an actual address of your dedicated mailbox):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

- When you select **Quarantine mailbox**, you need to specify message quarantine address (for example main_quarantine@company.com).

NOTE: The advantage of Quarantine mailbox / MS Exchange quarantine over Local quarantine is that mail quarantine items are managed from one place regardless of how many servers with Hub Transport Server role. There is however one downside of Quarantine mailbox / MS Exchange quarantine, SPAM and quarantined email messages are stored within Exchange mailbox database(s) and only administrator is able to manage the mail quarantine.

5.1.9.2.1 Quarantine manager settings

Host address - will appear automatically if your Exchange Server with CAS role is present locally. Alternatively, if CAS role is not present on the same server with ESET Mail Security installed but it can be found within AD, host address will appear automatically. If it does not appear, you can type the host name manually. Automatic detection will not work on Edge Transport Server role.

NOTE: IP address is not supported, you need to use host name of the CAS server.

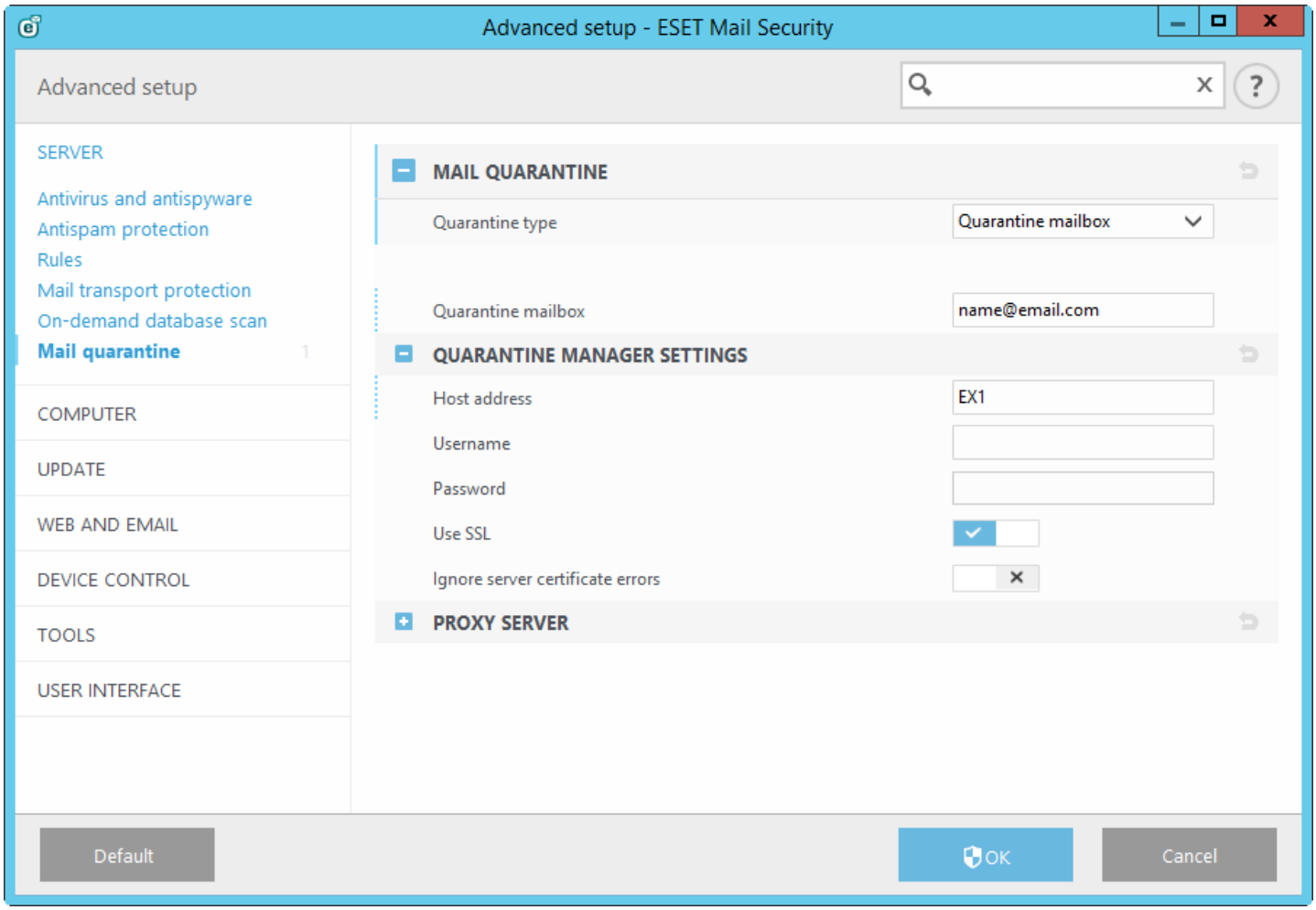
Username - dedicated quarantine user account you've created for storing quarantined messages (or an account that has access to this mailbox via access delegation). On Edge Transport Server role that is not part of the domain, it is necessary to use the whole email address (for example main_quarantine@company.com).

Password - type password of your quarantine account.

Use SSL - needs to be enabled if EWS (Exchange Web Services) is set to **Require SSL** in IIS. If SSL is enabled, Exchange Server certificate must be imported on the system with ESET Mail Security (in case Exchange Server roles are on different servers). Settings for the EWS can be found in IIS in *Sites/Default web site/EWS/SSL Settings*.

NOTE: Disable **Use SSL** only in case you have EWS configured in IIS not to Require SSL.

Ignore server certificate errors - Ignores following states: *self-signed, wrong name in certificate, wrong usage, expired*.



5.1.9.2.2 Proxy server

In case you use a proxy server between your Exchange Server with CAS role and Exchange Server where ESET Mail Security is installed, specify parameters of your proxy server. This is required because ESET Mail Security connects to EWS (Exchange Web Services) API via HTTP/HTTPS. Otherwise Quarantine mailbox and MS Exchange quarantine will not work.

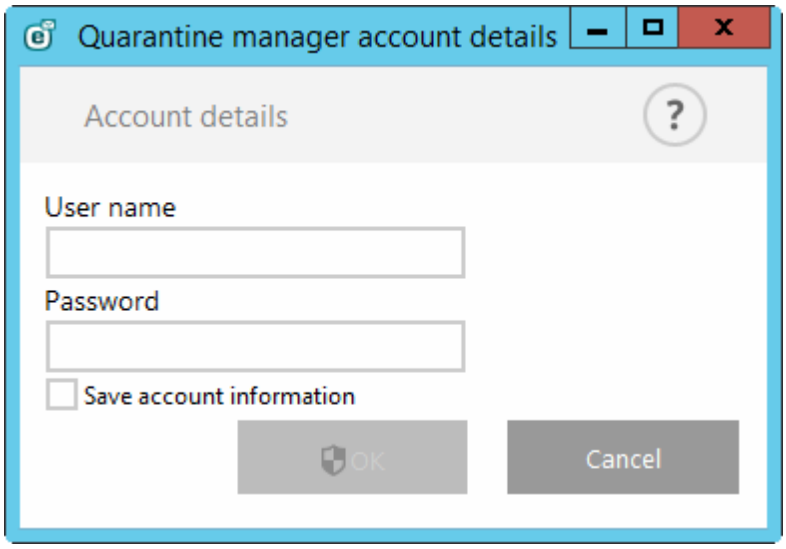
Proxy server - enter IP address or name of the proxy server you use.

Port - enter port number of the proxy server.

Username, Password - enter credentials if your proxy server requires authentication.

5.1.9.3 Quarantine manager account details

This dialog window will display if you do not setup an account for your **Quarantine manager details**. Specify credentials for a user with access to the **Quarantine mailbox** and click **OK**. Alternatively, press F5 to access **Advanced setup** and navigate to **Server** > **Mail Quarantine** > Quarantine manager settings. Type the **User name** and **Password** for your quarantine mailbox.



You can select **Save account information** to save account settings for future use when accessing Quarantine manager.

5.2 Computer

The **Computer** module can be found under **Setup** > **Computer**. It displays an overview of the protection modules described in the previous chapter. In this section, the following settings are available:

- Real-time file system protection
- On-demand computer scan
- Idle-state scanning
- Startup scan
- Removable media
- Document protection
- HIPS

Scanner options for all protection modules (for example Real-time file system protection, Web access protection, etc.) allow you to enable or disable detection of the following:

- Potentially unwanted applications (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way.
  Read more about these types of applications in the glossary.
- Potentially unsafe applications refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.
  Read more about these types of applications in the glossary.
- **Potentially suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

Anti-Stealth technology is a sophisticated system that detects dangerous programs such as rootkits which are able to hide themselves from the operating system, making it impossible to detect them using ordinary testing techniques.

Processes exclusions allows you to exclude specific processes. For example, processes of the backup solution, where all file operations attributed to such excluded processes are ignored and considered safe, minimizing

interference with the backup process.

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan. For instructions to exclude an object from scanning see Exclusions.

5.2.1 An infiltration is detected

Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, diskettes, etc.).

Standard behavior

As a general example of how infiltrations are handled by ESET Mail Security, infiltrations can be detected using:

- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

Each uses the standard cleaning level and will attempt to clean the file and move it to Quarantine or terminate the connection. A notification window is displayed in the notification area at the bottom right corner of the screen. For more information about cleaning levels and behavior, see Cleaning.

Cleaning and deleting

If there is no predefined action to take for Real-time file system protection, you will be prompted to select an option in the alert window. Usually the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, as this will leave infected files uncleaned. The exception to this is when you are sure that a file is harmless and has been detected by mistake.

Apply cleaning if a file has been attacked by a virus that has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

If an infected file is “locked“ or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Multiple threats

If any infected files were not cleaned during Computer scan (or the Cleaning level was set to **No Cleaning**), an alert window prompting you to select actions for those files is displayed. Select an action individually for each threat in the list or you can use **Select action for all listed threats** and choose one action to take on all the threats in the list, then click **Finish**.

Deleting files in archives

In Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a Strict cleaning scan, with Strict cleaning enabled an archive will be deleted if it contains at least one infected file regardless of the status of other files in the archive.
If your computer is showing signs of a malware infection, e.g., it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Mail Security and click Computer scan
- Click **Smart scan** (for more information, see Computer scan)
- After the scan has finished, review the log for the number of scanned, infected and cleaned files

If you only want to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

5.2.2 Processes exclusions

This feature allows you to exclude processes of applications from Antivirus on-access scanning. These exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications which in turn has a positive effect on the overall performance of the operating system.

When a process is excluded, it's executable file is not monitored. Activity of excluded process is not monitored by ESET Mail Security and no scanning is performed on any file operations performed by the process.

Use **Add**, **Edit** and **Remove** to manage Processes exclusions.

NOTE: Process exclusions are exclusions from Antivirus on-access scanning only. For example, Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend creating exclusions for web browsers.

NOTE: HIPS is involved in the evaluation of excluded processes, therefore we recommend that you test newly excluded processes with HIPS enabled (or disabled if you experience problems). Disabling HIPS will not affect process exclusions. If HIPS is disabled, the identification of excluded processes is based on path only.

5.2.3 Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from antivirus scans for most of their products. Antivirus scans may have a negative influence on a server's performance, lead to conflicts and even prevent some applications from running on the server. Exclusions help minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.

ESET Mail Security identifies critical server applications and server operating system files, and automatically adds them to the list of Exclusions. You can see a list of detected server applications under **Automatic exclusions to generate** for which exclusions were created. All automatic exclusions are enabled by default. You can disable/ enable each server application by clicking the switch with the following result:

1. If an application/operating system exclusion remains enabled, any of its critical files and folders will be added to the list of files excluded from scanning (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting if you want to make sure the recommended Automatic exclusions are always applied.
2. If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**). However, they will not be automatically checked and renewed on the **Exclusions** list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to remove the exclusions from the list without restarting the server, you will need to remove them manually from the list (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**).

Any user-defined exclusions entered manually (under **Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**) will not be affected by the settings described above.

The Automatic exclusions of server applications/operating systems are selected based on Microsoft's recommendations. For details, please see the following Microsoft Knowledge Base articles:

- Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows
- Recommendations for troubleshooting an Exchange Server computer with antivirus software installed
- File-Level Antivirus Scanning on Exchange 2007
- Anti-Virus Software in the Operating System on Exchange Servers

5.2.4 Shared local cache

The Shared local cache will boost performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. Turn on the **Caching option** switch to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET Mail Security will search for scanned files in the cache. If files match, they will be excluded from scanning.

Cache server setup contains the following**:**

- **Hostname** - Name or IP address of the computer where the cache is located.
- **Port** - Number of the port used for communication (same as was set in Shared local cache).
- **Password** - Specify the Shared local cache password if required.

5.2.5 Performance

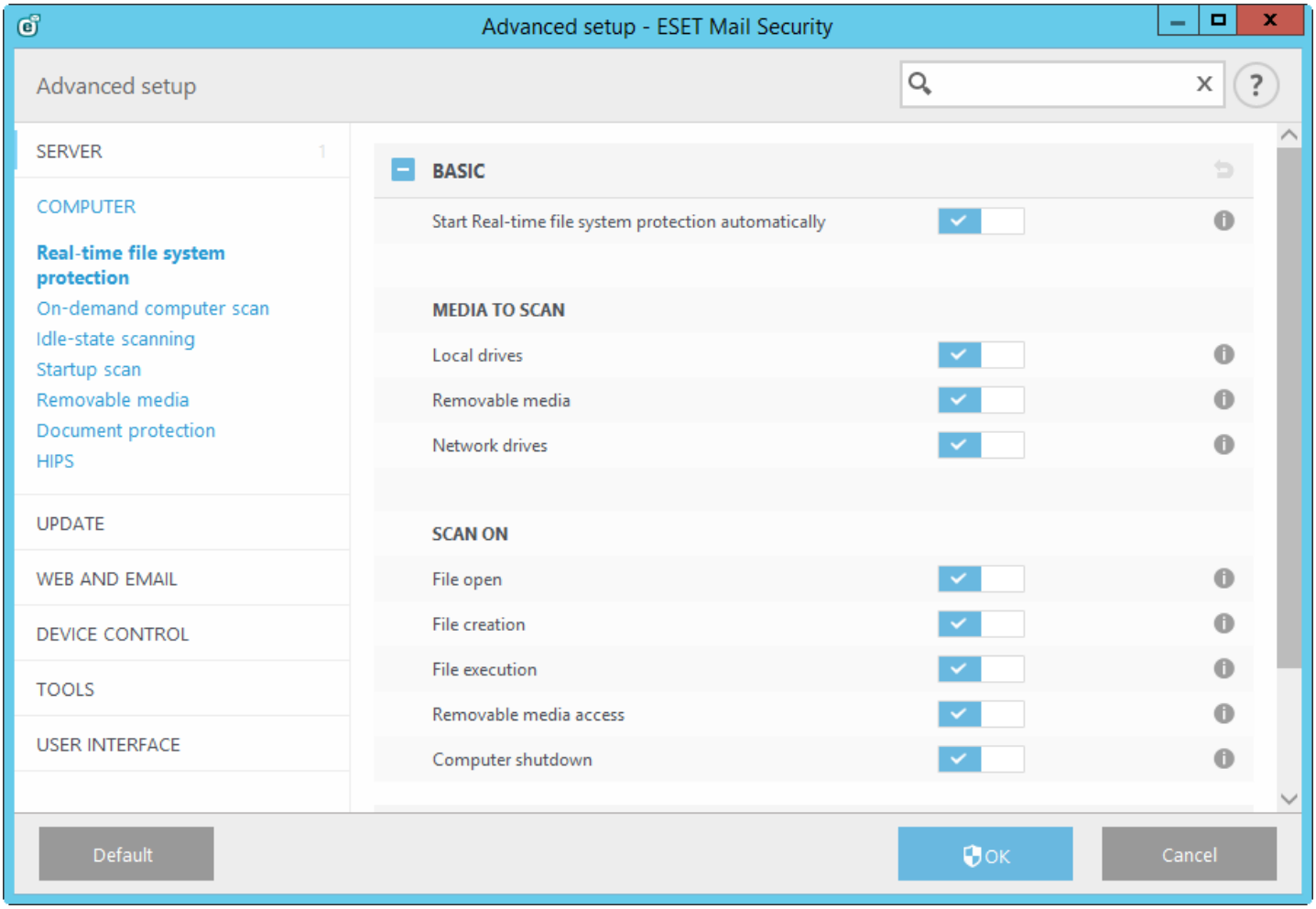
You can set a number of independent ThreatSense scan engines used by the antivirus and antispyware protection at a time.

If there are no other restrictions, we recommend you to increase the number of ThreatSense scan engines according to this formula: *number of ThreatSense scan engines = (number of physical CPUs x 2) + 1*.

NOTE: Acceptable value is 1-20, so the maximum number of ThreatSense scan engines you can use is 20.

5.2.6 Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. Real-time file system protection is launched at system startup.



By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In

special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging **Start Real-time file system protection automatically** in **Advanced setup** under **Real-time file system protection** > **Basic**.

- **Media to scan**

By default, all types of media are scanned for potential threats:

Local drives - Controls all system hard drives.
Removable media - Controls CD/DVDs, USB storage, Bluetooth devices, etc.
Network drives - Scans all mapped drives.

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

- **Scan on**

By default, all files are scanned upon opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open** - Enables or disables scanning when files are opened.
- **File creation** - Enables or disables scanning when files are created.
- **File execution** - Enables or disables scanning when files are run.
- **Removable media access** - Enables or disables scanning triggered by accessing particular removable media with storage space.
- **Computer shutdown** - Enables or disables scanning triggered by computer shutdown.

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in the ThreatSense parameters section), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is controlled using **Smart optimization**. If **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, press **F5** to open Advanced setup and expand **Computer** > **Real-time file system protection**. Click **ThreatSense parameters** > **Other** and select or deselect **Enable Smart optimization**.

5.2.6.1 Exclusions

Note to be confused with **Excluded extensions**

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan (for example, backup software).

To exclude an object from scanning:

Click **Add** and enter the path to an object or select it in the tree structure.
You can use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters.

Examples

- If you want to exclude all files in a folder, type the path to the folder and use the mask “*.*”.
- To exclude an entire drive including all files and subfolders, use the mask "D:*".
- If you want to exclude doc files only, use the mask “*.doc“.
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D????.exe”. Question marks replace the missing (unknown) characters.

NOTE: A threat within a file will not be detected by the Real-time file system protection module or Computer scan module if that file meets the criteria for exclusion from scanning.

Columns

Path - Path to excluded files and folders.
Threat - If the name of a threat is displayed next to an excluded file, it means that the file is only excluded for the given threat. If that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations, and can be created either in the threat alert window reporting the infiltration (click **More info** and then select **Exclude from detection**), or by clicking **Tools** > **Quarantine**, right-clicking the quarantined file and then selecting **Restore and exclude from scanning** from the context menu.

Control elements

Add - Excludes objects from detection.
Edit - Enables you to edit selected entries.
Remove - Removes selected entries.

5.2.6.1.1 Add or Edit exclusion

This dialog window enables you to add or edit exclusions. It can be done in two ways:

- by typing the path to an object to be excluded
- by selecting it in the tree structure (click the **...** at the end of the text field to browse)

If using the first method, wildcards described in the Exclusion format section can be used.

5.2.6.1.2 Exclusion format

You can use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters.

Examples

- If you want to exclude all files in a folder, type the path to the folder and use the mask “*.*”.
- To exclude an entire drive including all files and subfolders, use the mask "D:*".
- If you want to exclude doc files only, use the mask “*.doc“.
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D????.exe”. Question marks replace the missing (unknown) characters.

5.2.6.2 ThreatSense parameters

ThreatSense is technology comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

NOTE: For details about automatic startup file check, see Startup scan.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense engine parameter setup** in the Advanced setup window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

- **Operating memory** - Scans for threats that attack the operating memory of the system.
- **Boot sectors** - Scans boot sectors for the presence of viruses in the MBR (Master Boot Record). In case of a Hyper-V Virtual Machine, its disk MBR is scanned in read only mode.
- **Email files** - The program supports the following extensions: DBX (Outlook Express) and EML.
- **Archives** - The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.
- **Self-extracting archives** – Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.
- **Runtime packers** - After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

- **Heuristics** - A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.
- **Advanced heuristics/DNA/Smart signatures** - Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning:

No cleaning - Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning - The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program

provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning - The program will clean or delete all infected files. The only exceptions are system files. If it is not possible to clean a file, the user will be asked what type of action should be taken.

WARNING: If an archive contains a file or files that are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive will be deleted if all the files it contains are infected. In **Strict cleaning** mode, the archive will be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

IMPORTANT: If Hyper-V host is running on Windows Server 2008 R2, **Normal cleaning** and **Strict cleaning** are not supported. Scanning of Virtual Machine disks is done in read-only mode - **No cleaning**. Regardless of what Cleaning level is selected, the scan is always performed in read-only mode.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to exclude from scan.

Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in **Other** section are also available:

- **Scan alternate data streams (ADS)** - Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.
- **Run background scans with low priority** - Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.
- **Log all objects** - If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.
- **Enable Smart optimization** - With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.
- **Preserve last access timestamp** - Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Default object settings

- **Maximum object size** - Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.
- **Maximum scan time for object (sec.)** - Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive scan setup

Archive nesting level - Specifies the maximum depth of archive scanning. Default value: *10*.

Maximum size of file in archive - This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

NOTE: We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

5.2.6.2.1 File extenstions excluded from scanning

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

By default, all files are scanned. Any extension can be added to the list of files excluded from scanning.

Excluding files is sometimes necessary if scanning certain file types prevents the program that is using certain extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

Using the **Add** and **Remove** buttons, you can allow or prohibit the scanning of specific file extensions. To add a new extension to the list, click **Add** type the extension into the blank field and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons. When multiple selection is enabled, extensions will be shown in the list. Select an extension in the list and click **Remove** to delete that extension from the list. If you want to edit a selected extension click **Edit**.

The special symbol ? (question mark) can be used. The question mark represents any symbol.

5.2.6.2.2 Additional ThreatSense parameters

Additional ThreatSense parameters for newly created and modified files - The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the virus signature database update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

To learn more about **Runtime packers**, **Self-extracting archives** and **Advanced heuristics** see ThreatSense engine parameters setup.

Additional ThreatSense parameters for executed files - By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid enabled to mitigate impact on system performance.

5.2.6.2.3 Cleaning levels

Real-time protection has three cleaning levels (to access cleaning level settings, click **ThreatSense parameters** in the **Real-time file system protection** section and then click **Cleaning**).

No cleaning - Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning - The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning - The program will clean or delete all infected files. The only exceptions are system files. If it is not possible to clean a file, the user will be asked what type of action should be taken.

WARNING: If an archive contains a file or files that are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive will be deleted if all the files it contains are infected. In **Strict cleaning** mode, the archive will be deleted if it contains at least one infected file, regardless of

the status of the other files in the archive.

IMPORTANT: If Hyper-V host is running on Windows Server 2008 R2, **Normal cleaning** and **Strict cleaning** are not supported. Scanning of Virtual Machine disks is done in read-only mode - **No cleaning**. Regardless of what Cleaning level is selected, the scan is always performed in read-only mode.

5.2.6.2.4 When to modify real-time protection configuration

Real-time file system protection is the most essential component for maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET Mail Security, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click next to each tab in the window (**Advanced setup** > **Computer** > **Real-time file system protection**).

5.2.6.2.5 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file is available for download at http://www.eicar.org/download/eicar.com

5.2.6.2.6 What to do if real-time protection does not work

In this chapter, we describe problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** in the main program window and click **Real-time file system protection**.

If real-time protection is not initiated at system startup, it is usually because **Start Real-time file system protection automatically** is deselected. To enable this option, navigate to Advanced setup (**F5**) and click **Computer** > **Real-time file system protection** > **Basic** in the **Advanced setup** section. Make sure that **Start Real-time file system protection automatically** is turned on.

If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system before installing ESET.

Real-time protection does not start

If real-time protection is not initiated at system startup (and **Start Real-time file system protection automatically** is enabled), it may be due to conflicts with other programs. For assistance resolving this issue, please contact ESET Customer Care.

5.2.6.2.7 Submission

You can select how files and statistical information will be submitted to ESET. Select the **By means of Remote Administrator or directly to ESET** option for files and statistics to be submitted by any available means. Select the **By means of Remote Administrator** option to submit files and statistics to the remote administration server, which will ensure their subsequent submission to the ESET Threat Lab. If **Directly to ESET** is selected, all suspicious files and statistical information are sent to the ESET virus lab directly from the program.

When there are files pending submission, the **Submit now** button will be active. Click this button to immediately submit files and statistical information.

Select **Enable logging** to create a log to record file and statistical information submissions.

5.2.6.2.8 Statistics

The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats. This information may include the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. The statistics are typically delivered to ESET servers once or twice a day.

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

When to submit - You can define when the statistical information will be submitted. If you choose to submit **As soon as possible**, statistical information will be sent immediately after it is created. This setting is suitable if a permanent Internet connection is available. If **During update** is selected, statistical information will be submitted collectively during the next update.

5.2.6.2.9 Suspicious files

The **Suspicious files** tab allows you to configure the manner in which threats are submitted to the ESET Threat Lab for analysis.

If you find a suspicious file, you can submit it for analysis to our ThreatLabs. If it is a malicious application, its detection will be added to the next virus signature update.

File submission can be set to occur automatically, or select **Ask before submitting** if you want to know which files have been sent for analysis and confirm the submission.

If you do not want any files to be submitted, select the **Do not submit for analysis** option. Selecting not to submit files for analysis does not affect submission of statistical information which is configured in its own setup (see section Statistics).

When to submit - By default, the **As soon as possible** option is selected for suspicious files to be sent to ESET's Threat Lab. This is recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. Select the **During** update option for suspicious files to uploaded to ThreatSense.Net during the next update.

Exclusion filter - The Exclusion filter allows you to exclude certain files/folders from submission. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

Contact email - Your **Contact email [optional]** can sent with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

5.2.7 On-demand computer scan and Hyper-V scan

This section provides options to select scanning parameters.

NOTE: This scan profile selector applies to both On-demand computer scan and Hyper-V scan.

Selected profile - A particular set of parameters used by the on-demand scanner. To create a new one, click **Edit** next to **List of profiles**.

If only want to scan a specific target, you can click **Edit** next to **Scan targets** and choose an option from drop-down menu or selecting specific targets from the folder (tree) structure.

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

Click ThreatSense parameters to modify scan parameters (for example, detection methods) for the On-demand computer scanner.

5.2.7.1 Custom scan and Hyper-V scan launcher

If only want to scan a specific target, you can use the Custom scan tool by clicking **Computer scan** > **Custom scan** and selecting an option from the **Scan targets** drop-down menu or selecting specific targets from the folder (tree) structure.

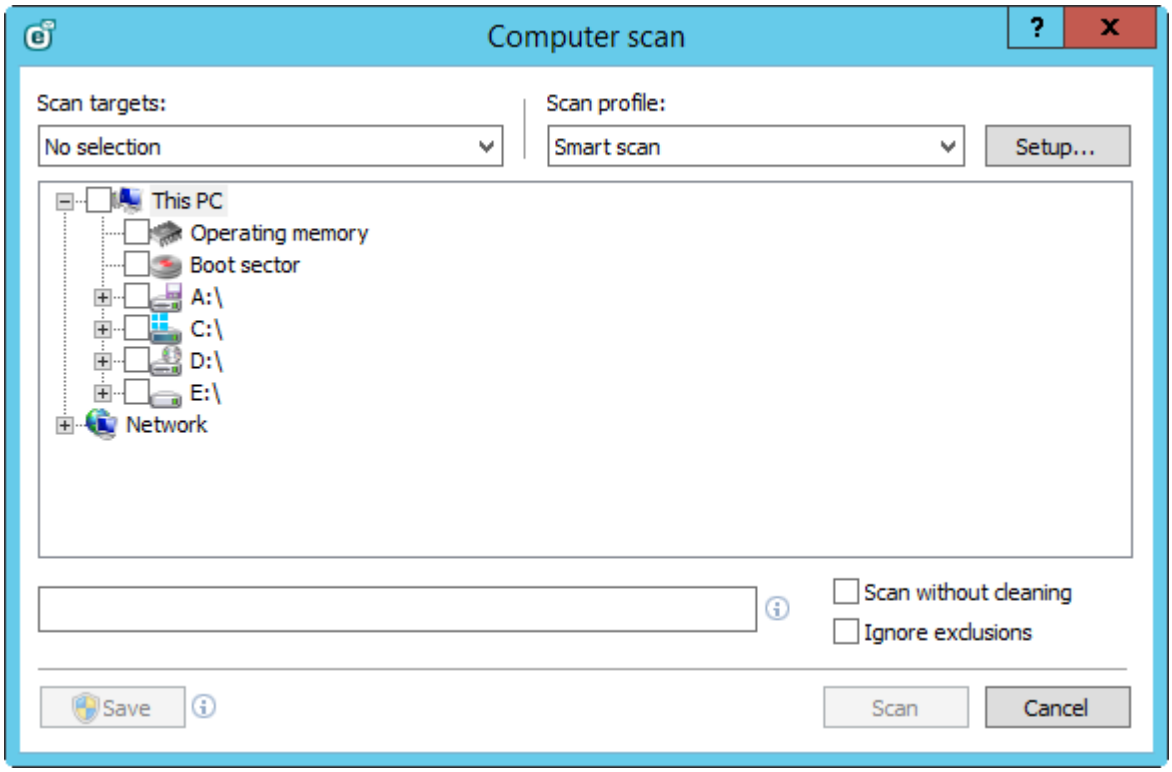
NOTE: This scan target selector applies to both Custom scan and Hyper-V scan.

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

To quickly navigate to a scan target or to directly add a desired target (folder or file(s)), enter it in the blank field below the folder list. This is only possible if no targets were selected in the tree structure and the **Scan targets** menu is set to **No selection**.

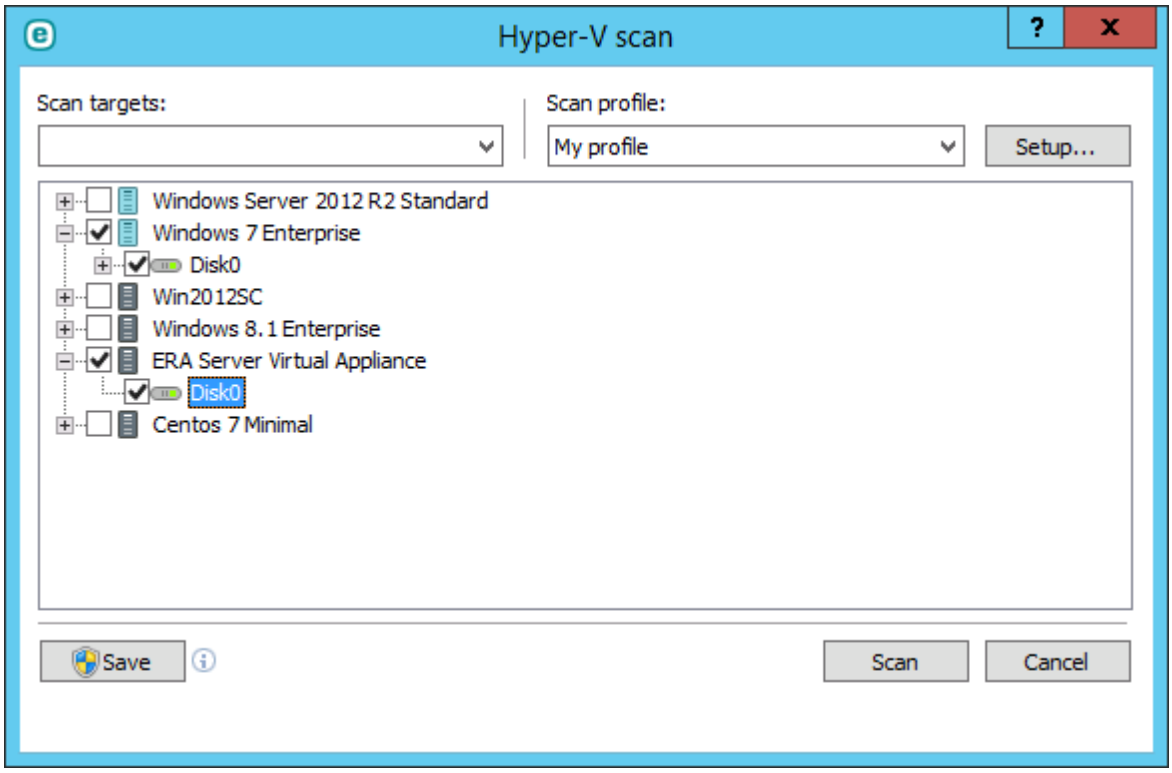
Custom scan pop-up window:



If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. This is useful when you only want to obtain an overview whether there are infected items and get details about these infections, if there are any. Furthermore, you can choose from three cleaning levels by clicking **Setup** > **ThreatSense parameters** > **Cleaning**. Information about scanning is saved to a scan log.

When you select **Ignore exclusions**, it lets you perform a scan while ignoring exclusions that otherwise apply.

Hyper-V scan pop-up window (see Hyper-V scan for more information):



You can choose a profile from the **Scan profile** drop-down menu to be used for scanning chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense engine parameters. Click **Setup...** to set up chosen scan profile from the Scan profile menu in detail. The available options are described under section **Other** in ThreatSense engine parameters setup.

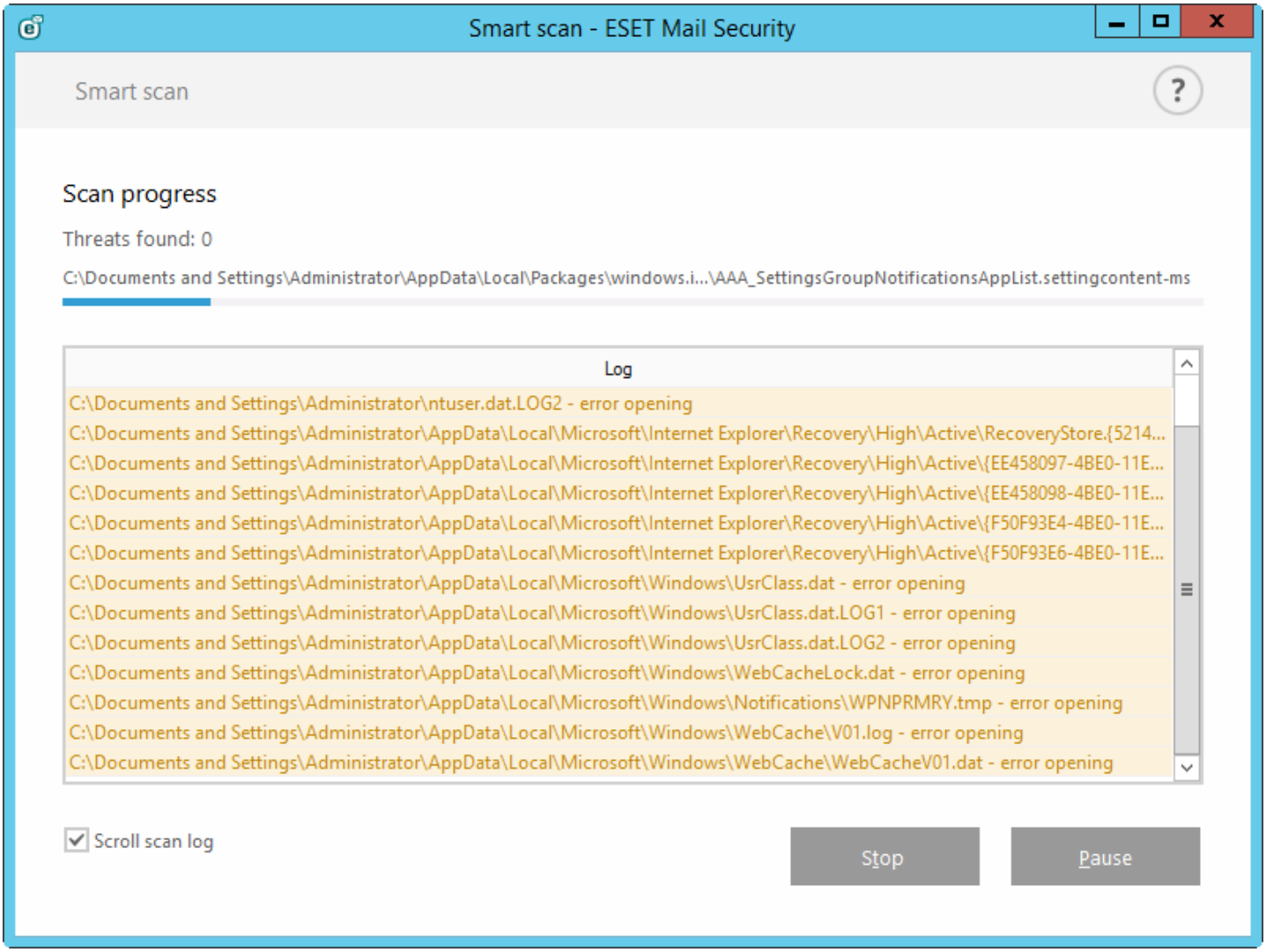
Click **Save** to save changes made to your target selection, including selections made within the folder tree structure.

Click **Scan** to execute the scan using the custom parameters that you have set.

Scan as Administrator allows you to execute the scan under the Administrator account. Click this if the current user doesn't have privileges to access the appropriate files to be scanned. Note that this button is not available if the current user cannot call UAC operations as Administrator.

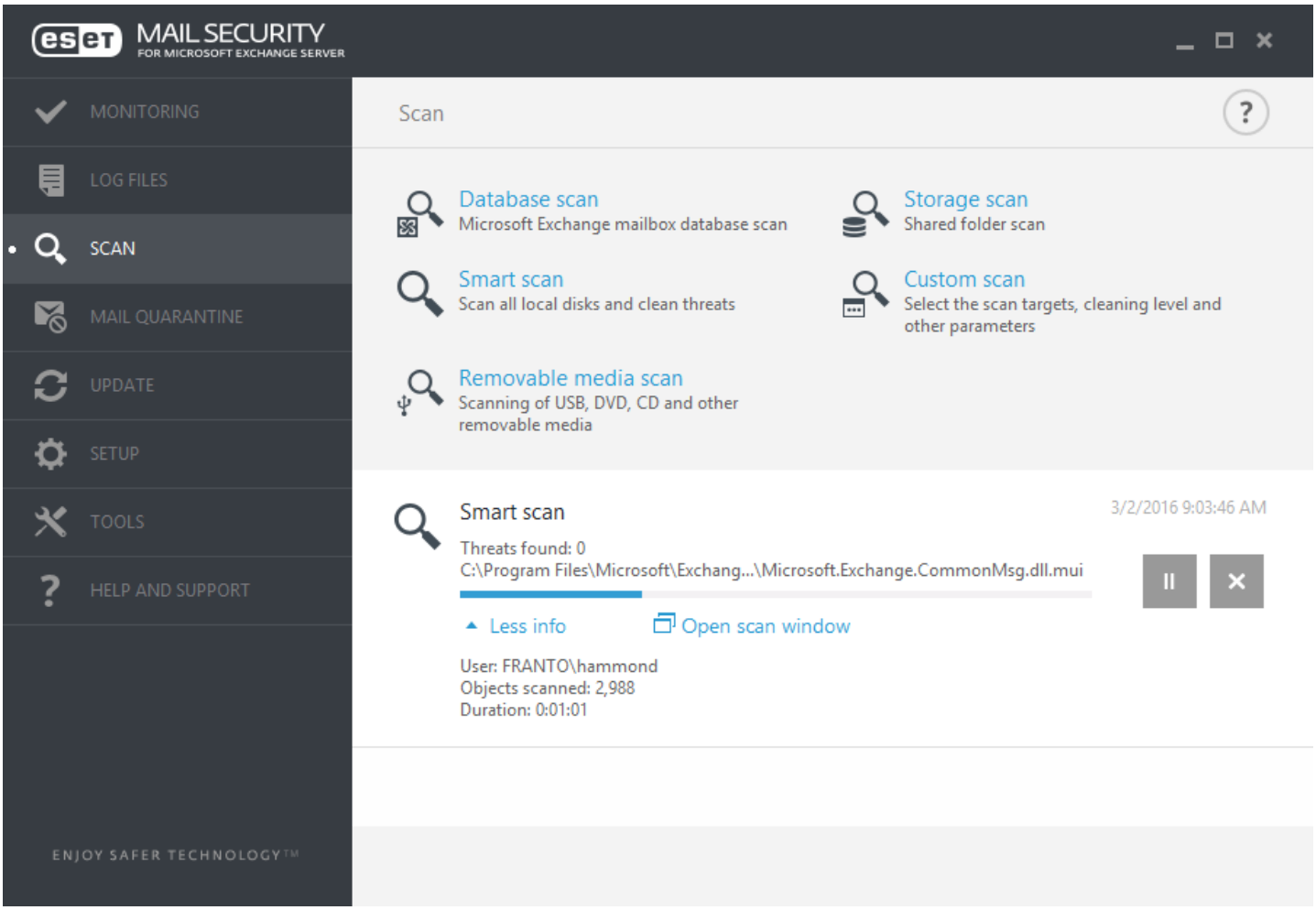
5.2.7.2 Scan progress

The scan progress window shows the current status of the scan and information about the number of files found that contain malicious code.


Smart scan - ESET Mail Security
Smart scan
Scan progress
Threats found: 0
C:\Documents and Settings\Administrator\AppData\Local\Packages\windows.i...\AAA_SettingsGroupNotificationsAppList.settingcontent-ms
Log
C:\Documents and Settings\Administrator\ntuser.dat.LOG2 - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5214...
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EE458097-4BE0-11E...
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EE458098-4BE0-11E...
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F50F93E4-4BE0-11E...
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F50F93E6-4BE0-11E...
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\WebCacheLock.dat - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\Notifications\WPNPRMRY.tmp - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\WebCache\V01.log - error opening
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat - error opening
Scroll scan log
Stop
Pause

NOTE: It is normal that some files, such as password protected files or files exclusively being used by the system (typically *pagefile.sys* and certain log files), cannot be scanned.

Scan progress - The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.
Target - The name of the currently scanned object and its location.
Threats found - Shows the total number of threats found during a scan.
Pause - Pauses a scan.
Resume - This option is visible when scan progress is paused. Click Resume to continue scanning.
Stop - Terminates the scan.
Scroll scan log - If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.



You can click **More info** during the scan progress to see details such as the **User** who executed scan process from GUI, a number of **Objects scanned** and the scan **Duration**. If On-demand **Database scan** is running, it shows the user who executed the scan, not the actual Database scan account that is being used to connect to EWS (Exchange Web Services) during the scan process.

5.2.7.3 Profile manager

Profile manager is used in two places within ESET Mail Security - in the **On-demand computer scan** section and in the **Update** section.

On-demand computer scan

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced setup window (F5) and click **Computer** > **On-demand computer scan** and then **Edit** next to **List of profiles**. The **Selected profile** drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Example: Suppose that you want to create your own scan profile and the Smart scan configuration is partially

suitable, but you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. Enter the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements and click **OK** to save your new profile.

Update

The profile editor in the Update setup section allows users to create new update profiles. Create and use your own custom profiles (other than the default **My profile**) only if your computer uses multiple means to connect to update servers.

For example, a laptop that normally connects to a local server (Mirror) in the local network but downloads updates directly from ESET update servers when disconnected from the local network (business trip) might use two profiles: the first one for connecting to the local server; the other one for connecting to ESET servers. Once these profiles are configured, navigate to **Tools** > **Scheduler** and edit the update task parameters. Designate one profile as primary and the other as secondary.

Selected profile - The currently used update profile. To change it, choose a profile from the drop-down menu.

List of profiles - Create new or edit update profiles.

5.2.7.4 Scan targets

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

5.2.7.5 Pause a scheduled scan

The scheduled scan can be postponed. Set a value for the **Stop scheduled scans in (min)** option, if you wish to postpone the computer scan.

5.2.8 Idle-state scanning

You can enable the idle-state scanner in **Advanced setup** under **Computer** > **Idle-state scanning** > **Basic**. Set the switch next to **Enable Idle-state scanning** to **On** to enable this feature. When the computer is in idle state, a silent computer scan is performed on all local drives.

By default, the Idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting by selecting the check box next to **Run even if computer is powered from battery** in Advanced setup.

Turn on the **Enable logging** switch in Advanced setup to record a computer scan output in the Log files section (from the main program window click **Tools** > **Log files** and select **Computer scan** from the **Log** drop-down menu).

Idle-state detection will run when your computer is in the following states:

- Turned off screen or screen saver
- Computer lock
- User logoff

Click ThreatSense parameters to modify scan parameters (for example, detection methods) for the Idle-state scanner.

5.2.9 Startup scan

By default, the automatic startup file check will be performed on system startup and during virus signature database updates. This scan is controlled by the Scheduler configuration and tasks.

Startup scan options are a part of the **System startup file check** scheduler task. To modify Startup scan settings, navigate to **Tools** > **Scheduler**, click **Automatic startup file check** and then click **Edit**. In the last step, the Automatic startup file check window will appear (see the following chapter for more details).

For detailed instructions about Scheduler task creation and management, see Creating new tasks.

5.2.9.1 Automatic startup file check

When creating a System startup file check scheduled task, you have several options to adjust the following parameters:

The **Scan level** drop-down menu specifies the scan depth for files run at system startup. Files are arranged in ascending order according to the following criteria:

- **Only the most frequently used files** (least files scanned)
- **Frequently used files**
- **Commonly used files**
- **Rarely used files**
- **All registered files** (most files scanned)

Two specific **Scan level** groups are also included:

- **Files run before user logon** - Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll's, etc.).
- **Files run after user logon** - Contains files from locations that may only be accessed after a user has logged in (includes files that are only run by a specific user, typically files in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Lists of files to be scanned are fixed for each aforementioned group.

Scan priority - The level of priority used to determine when a scan will start:

- **Normal** - at an average system load,
- **Lower** - at a low system load,
- **Lowest** - when the system load is the lowest possible,
- **When idle** - the task will be performed only when the system is idle.

5.2.10 Removable media

ESET Mail Security provides automatic removable media (CD/DVD/USB) scanning. This module allows you to scan inserted media. This may be useful if the computer administrator wants to prevent the users from using removable media with unsolicited content.

Action to take after inserting removable media - Select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). If **Show scan options** is selected, a notification will display which allows you to choose a desired action:

- **Do not scan** - No action will be performed and the **New device detected** window will be closed.
- **Automatic device scan** - An on-demand computer scan of the inserted removable media device will be performed.
- **Show scan options** - Opens the Removable media setup section.

When removable media is inserted, the following dialog will shown:

- **Scan now** - This will trigger a scan of removable media.
- **Scan later** - Scanning of removable media will be postponed.
- **Setup** - Opens Advanced setup.
- **Always use the selected option** - When selected, the same action will be performed when removable media is inserted another time.

In addition, ESET Mail Security features the Device control functionality, which allows you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

5.2.11 Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that are not exposed to a high volume of Microsoft Office documents.

- **Integrate into system** activates the protection system. To modify this option, press **F5** to open the Advanced setup window and click **Computer** > **Document protection** in the Advanced setup tree.
- See Threatsense parameters for more information about Document protection settings.

This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

5.2.12 HIPS

Changes to HIPS settings should only be made by an experienced user. Incorrect configuration of HIPS settings can lead to system instability.

Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

HIPS settings can be found in **Advanced setup** (F5) > **Computer** > **HIPS**. The HIPS state (enabled/disabled) is shown in the ESET Mail Security main program window, in the **Setup** pane, on the right side of the **Computer** section.

ESET Mail Security has built-in *Self-defense* technology that prevents malicious software from corrupting or disabling your antivirus and antispyware protection, so you can be sure your system is protected at all times. Changes to the **Enable HIPS** and **Enable SD (Self-Defense)** settings take effect after the Windows operating system is restarted. Disabling the entire **HIPS** system will also require a computer restart.

Advanced Memory Scanner works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced Memory Scanner is enabled by default. Read more about this type of protection in the glossary.

Exploit Blocker is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit Blocker is enabled by default. Read more about this type of protection in the glossary.

Filtering can be performed in one of four modes:

- **Automatic mode** - Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.
- **Smart mode** - The user will only be notified about very suspicious events.
- **Interactive mode** - The user will be prompted to confirm operations.
- **Policy-based mode** - Operations are blocked.
- **Learning mode** - Operations are enabled and a rule is created after each operation. Rules created in this mode can

be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select Learning mode from the HIPS Filtering mode drop down menu, the **learning mode will end at** setting will become available. Select the duration for which you want to engage learning mode (the maximum duration is 14 days). When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to the rules used by the personal firewall. Click **Edit** to open the HIPS rule management window. Here you can select, create, edit or delete rules. More details on rule creation and HIPS operations can be found in the Edit rule chapter.

If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered. You can choose to **Block** or **Allow** the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

The dialog window allows you to create a rule based on any new action that HIPS detects and then define the conditions under which to allow or block that action. Settings for the exact parameters can be accessed by clicking **Show Options**. Rules created like this are considered equal to rules created manually, so a rule created from a dialog window can be less specific than the rule that triggered that dialog window. This means that after creating such a rule, the same operation can trigger the same window.

Temporarily remember this action for this process causes the action (**Allow/Block**) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

5.2.12.1 HIPS rules

This window gives you an overview of existing HIPS rules.

Columns

Rule - User-defined or automatically chosen rule name.
Enabled - Deactivate this switch if you want to keep the rule in the list but do not want to use it.
Action - The rule specifies an action - **Allow**, **Block** or **Ask** - that should be performed if the conditions are right.
Sources - The rule will be used only if the event is triggered by an application(s).
Targets - The rule will be used only if the operation is related to a specific file, application or registry entry.
Log - If you activate this option, information about this rule will be written to the HIPS log.
Notify - A small pop-up window appears in the lower-right corner if an event is triggered.

Control elements

Add - Creates a new rule.
Edit - Enables you to edit selected entries.
Remove - Removes selected entries.

5.2.12.1.1 HIPS rule settings

- **Rule name** - User-defined or automatically chosen rule name.
- **Action** - The rule specifies an action - **Allow**, **Block** or **Ask** - that should be performed if the conditions are right.

Operations affecting - You must select the type of operation for which the rule will be applied. The rule will be used only for this type of operation and for the selected target.

- **Files** - The rule will be used only if the operation is related to this target. Select Specific files from drop-down menu and click Add to add new files or folders or you can select All files from drop-down menu to add all applications.
- **Applications** - The rule will be used only if the event is triggered by this application(s). Select Specific applications from drop-down menu and click Add to add new files or folders or you can select All applications from drop-down menu to add all applications.
- **Registry entries** - The rule will be used only if the operation is related to this target. Select Specific entries from drop-down menu and click Add to add new files or folders or you can select All entries from drop-down menu to add all applications.
- **Enabled** - Deactivate this switch if you wish to keep the rule in the list but do not wish to use it.
- **Log** - If you activate this option, information about this rule will be written to the HIPS log.
- **Notify user** - A small pop-up window appears in the lower-right corner if an event is triggered.

The rule consists of parts that describe the conditions triggering this rule:

Source applications - The rule will be used only if the event is triggered by this application(s).Select **Specific applications** from drop-down menu and click **Add** to add new files or folders or you can select **All applications** from the drop-down menu to add all applications.
Files - The rule will be used only if the operation is related to this target. Select **Specific files** from drop-down menu and click **Add** to add new files or folders or you can select **All files** from the drop-down menu to add all applications.
Applications - The rule will be used only if the operation is related to this target. Select **Specific applications** from the drop-down menu and click **Add** to add new files or folders or you can select **All applications** from the drop-down menu to add all applications.
Registry entries - The rule will be used only if the operation is related to this target. Select **Specific entries** from the drop-down menu and click **Add** to add new files or folders, or you can select **All entries** from the drop-down menu to add all applications.

Descriptions of important operations:

File operations

- **Delete file** - Application is asking for permission to delete the target file.
- **Write to file** - Application is asking for permission to write to the target file.
- **Direct access to disk** - Application is trying to read from or write to the disk in a non-standard way that will circumvent common Windows procedures. This may result in files being modified without the application of corresponding rules. This operation may be caused by malware trying to evade detection, backup software trying to make an exact copy of a disk, or a partition manager trying to reorganize disk volumes.
- **Install global hook** - Refers to calling the SetWindowsHookEx function from the MSDN library.
- **Load driver** - Installation and loading of drivers onto the system.

Application operations

- **Debug another application** - Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified and its data can be accessed.
- **Intercept events from another application** - The source application is attempting to catch events targeted at a specific application (for example a keylogger trying to capture browser events).
- **Terminate/suspend another application** - Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes pane).
- **Start new application** - Starting of new applications or processes.
- **Modify state of another application** - The source application is attempting to write into the target applications' memory or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

Registry operations

- **Modify startup settings** - Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the Run key in the Windows Registry.
- **Delete from registry** - Deleting a registry key or its value.
- **Rename registry key** - Renaming registry keys.
- **Modify registry** - Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or group rights for registry keys.

NOTE: You can use wildcards with certain restrictions when entering a target. Instead of a particular key the * (asterisk) symbol can be used in registry paths. For example *HKEY_USERS*\software* can mean *HKEY_USER\.default \software* but not *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** is not a valid registry key path. A registry key path containing *** defines "this path, or any path on any level after that symbol". This is the only way of using wildcards for file targets. First, the specific part of a path will be evaluated, then the path following the wildcard symbol (*).

If you create a very generic rule, the warning about this type of rule will be shown.

5.2.12.2 Advanced setup

The following options are useful for debugging and analyzing an application's behavior:

Drivers always allowed to load - Selected drivers are always allowed to load regardless of configured filtering mode, unless explicitly blocked by user rule.

Log all blocked operations - All blocked operations will be written to the HIPS log.

Notify when changes occur in Startup applications - Displays a desktop notification each time an application is added to or removed from system startup.

Please see the our Knowledgebase article for an updated version of this help page.

5.2.12.2.1 Drivers always allowed to load

Drivers shown in this list will always be allowed to load regardless of HIPS filtering mode, unless explicitly blocked by user rule.

Add - Adds a new driver.
Edit - Edit the path for a selected driver.
Remove - Removes a driver from the list.
Reset - Reloads a set of system drivers.

NOTE: Click **Reset** if you do not want drivers that you have added manually to be included. This can be useful if you have added several drivers and you cannot delete them from the list manually.

5.3 Update

Update setup options are available in the **Advanced setup** tree (F5) under **Update** > **General**. This section specifies update source information like the update servers being used and authentication data for these servers.

General

The update profile that is currently in use is displayed in the **Selected profile** drop-down menu. To create a new profile, click **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**.

If you experience problems with an update, click **Clear** to clear the temporary update cache.

Outdated virus signature database alerts

Set maximum database age automatically - Allows to set maximum time (in days) after which the virus signature database will be reported as out of date. Default value is 7.

- **Rollback**

If you suspect that a new update of the virus database and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET Mail Security records snapshots of virus signature database and program modules for use with the *rollback* feature. In order to create virus database snapshots, leave the **Create snapshots of update files** switch enabled. The **Number of locally stored snapshots** field defines the number of previous virus database snapshots stored.

If you click **Rollback** (**Advanced setup** (F5) > **Update** > **General**), you have to select a time interval from the drop-down menu that represents the period of time that the virus signature database and program module updates will be paused.

For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the Internet (for example, HTTP communication).

By default, the **Update type** (located under **Basic**) is set to **Regular update** to ensure that update files will automatically be download from the ESET server with the least network traffic.

Basic

Disable display notification about successful update - Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running. Please note that Presentation mode will turn off all notifications.

The **Update server** menu is set to AUTOSELECT by default. The Update server is the location where updates are stored. If you use an ESET server, we recommend that you leave the default option selected. If you were using custom update server and want to change it back to default, type in **AUTOSELECT**. ESET Mail Security will automatically choose ESET update servers.

When using a local HTTP server - also known as a Mirror - the update server should be set as follows:
http://computer_name_or_its_IP_address:2221

When using a local HTTP server with SSL - the update server should be set as follows:
https://computer_name_or_its_IP_address:2221

When using a local shared folder - the update server should be set as follows:
\\computer_name_or_its_IP_address\shared_folder

- **Updating from Mirror**

Authentication for update servers is based on the **Licensing key** generated and sent to you after purchase. When using a local Mirror server, you can define credentials for clients to log in to the Mirror server before receiving updates. By default, no verification is required and the **Username** and **Password** fields are left empty.

5.3.1 Update rollback

If you click **Rollback** (**Advanced setup** (F5) > **Update** > **Profile**), you have to select a time interval from the drop-down menu that represents the period of time that the virus signature database and program module updates will be paused.

Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. Because it represents a potential security risk, we do not recommend selecting this option.

The virus signature database version is downgraded to the oldest available and stored as a snapshot in the local computer file system.

Example: Let the number 10646 be the most recent version of virus signature database. 10645 and 10643 are stored as a virus signature database snapshots. Note that 10644 is not available because, for example, the computer was turned off and a more recent update was made available before 10644 was downloaded. If the **Number of locally stored snapshots** field is set to 2 and you click **Rollback**, the virus signature database (including program modules) will be restored to version number 10643. This process may take some time. Check whether the virus signature database version has downgraded from the main program window of ESET Mail Security in the Update section.

5.3.2 Update mode

The **Update mode** tab contains options related to the program component update. The program enables you to predefine its behavior when a new program component upgrade is available.

Program component updates brings new features or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required. In the **Program component update** section, three options are available:

- **Ask before downloading program components** - The default option. You will be prompted to confirm or refuse program component updates when they are available.
- **Always update program components** - A program component update will be downloaded and installed automatically. Please remember that a computer restart may be required.
- **Never update program components** - Program component updates will not be performed at all. This option is suitable for server installations, since servers can usually be restarted only when they are undergoing maintenance.

NOTE: Selecting the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers - for example, restarting the server automatically after a program update could cause serious damage.

If the **Ask before downloading update** option is active, a notification will display when a new update is available.

If the update file size is greater than the value specified in the **Ask if an update file is greater than (kB)** field, the program will display a notification.

5.3.3 HTTP Proxy

To access the proxy server setup options for a given update profile, click **Update** in the **Advanced setup** tree (F5) and then click **HTTP Proxy**. Click the **Proxy mode** drop-down menu and select one of the three following options:

- Do not use proxy server
- Connection through a proxy server
- Use global proxy server settings

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified in the **Tools** > **Proxy server** branch of the Advanced setup tree.

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET Mail Security.

The **Connection through a proxy server** option should be selected if:

- A proxy server should be used to update ESET Mail Security that is different from the proxy server specified in the global settings (**Tools** > **Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port** (3128 by default), plus **Username** and **Password** for the proxy server if required.
- The proxy server settings were not set globally, but ESET Mail Security will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. The settings are taken from Internet Explorer during program installation, but if they are subsequently changed (e.g. if you change your ISP), please check that the HTTP proxy settings listed in this window are correct. Otherwise the program will not be able to connect to the update servers.

The default setting for the proxy server is **Use global proxy server settings**.

NOTE: Authentication data such as **Username** and **Password** is intended for accessing the proxy server. Complete these fields only if a username and password are required. Please note that these fields are not for your Username/ Password for ESET Mail Security, and should only be completed if you know you need a password to access the Internet via a proxy server.

5.3.4 Connect to LAN as

When updating from a local server with a version of the Windows NT operating system, authentication for each network connection is required by default.

To configure such an account, select from the **Local user type** drop-down menu:

- **System account (default)**
- **Current user**
- **Specified user**

Select **System account (default)** to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select **Specified user** if you want the program to use a specific user account for authentication. Use this method when the default system account connection fails. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

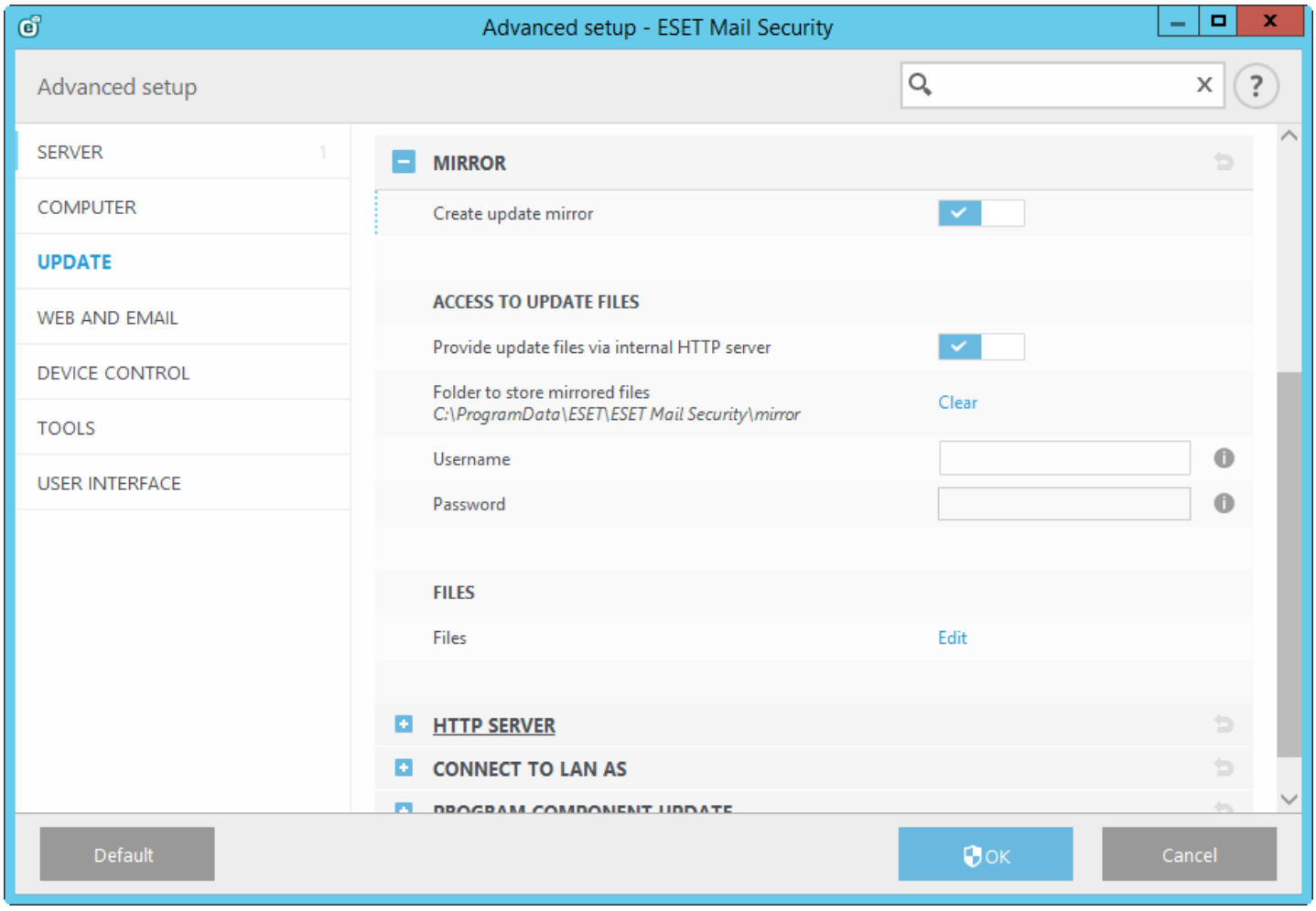
WARNING: When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend entering the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: *domain_name**user* (if it is a workgroup, enter *workgroup_name**name*) and password. When updating from the HTTP version of the local server, no authentication is required.

Engage **Disconnect from server after update** to force a disconnection if a connection to the server remains active even after updates have been downloaded.

5.3.5 Mirror

ESET Mail Security allows you to create copies of update files that can be used to update other workstations on the network. The use of a *"mirror"* - a copy of the update files in the LAN environment is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each workstation. Updates are downloaded to the local mirror server and then distributed to all workstations to avoid the risk of network traffic overload. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are located in Advanced setup under **Update.** To access this section press **F5** to access Advanced setup, click **Update** and select the **Mirror** tab.



To create a mirror on a client workstation, enable **Create update mirror**. Enabling this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

Access to update files

Provide update files via the internal HTTP server - If enabled, update files can be accessed through HTTP, no credentials are required.

NOTE: Windows XP requires service pack 2 or later to use the HTTP server.

Methods to access the Mirror server are described in detail in Updating from the Mirror. There are two basic methods for accessing the Mirror - the folder with update files can be presented as a shared network folder, or clients can access the mirror located on an HTTP server.

The folder dedicated to storing update files for the Mirror is defined under **Folder to store mirrored files**. Click **Folder** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be entered in the **Username** and **Password** fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder. The username and password should be

entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

Files - When configuring the Mirror you can specify the language versions of updates you want to download. Languages selected must be supported by the mirror server configured by the user.

HTTP server

Server port - By default, the Server port is set to 2221.

Authentication - Defines the method of authentication used for accessing update files. The following options are available: **None**, **Basic** and **NTLM**. Select **Basic** to use base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **NONE**, which grants access to the update files with no need for authentication.

Append your **Certificate chain file**, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: ASN, PEM and PFX. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. The **Private key type** option is set to **Integrated** by default (and therefore the **Private key file** option is disabled by default). This means that the private key is a part of the selected certificate chain file.

Connect to LAN as

Local user type - The **System account (default)**, **Current user**, and **Specified user** settings will be displayed in their corresponding drop-down menus. **Username** and **Password** settings are optional. See Connect to LAN as.

Select **Disconnect from server after update** to force a disconnection if a connection to the server remains active after updates have been downloaded.

Program component update

Automatically update components - Allows for the installation of new features and updates to existing features. An update can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required.

Update components now - Updates your program components to the latest version.

5.3.5.1 Updating from the Mirror

There are two basic methods to configure a Mirror, which is essentially a repository where clients can download update files. The folder with update files can be presented as a shared network folder or as an HTTP server.

Accessing the Mirror using an internal HTTP server

This configuration is the default, specified in the predefined program configuration. To allow access to the Mirror using the HTTP server, navigate to **Advanced setup** > **Update** > **Mirror** and select **Create update mirror**.

In the **HTTP Server** section of the **Mirror** tab you can specify the **Server port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **None**, **Basic**, and **NTLM**.

- Select **Basic** to use base64 encoding with basic username and password authentication.
- The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used.
- The default setting is **None**, which grants access to the update files with no need for authentication.

WARNING: If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Mail Security instance creating it.

SSL for HTTP Server

Append your **Certificate chain file**, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: **PEM, PFX** and **ASN**. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. **Private key type** is set to **Integrated** by default, which means that the private key is a part of the selected certificate chain file.

NOTE: An error **Invalid Username and/or Password** will appear in the Update pane from the main menu after several unsuccessful attempts to update the virus signature database from the Mirror. We recommend that you navigate to **Advanced setup** > **Update** > **Mirror** and check the Username and Password. The most common reason for this error is incorrectly entered authentication data.

After your Mirror server is configured, you must add the new update server on client workstations. To do this, follow the steps below:

- Access **Advanced setup** (F5) and click **Update** > **Basic**.
- Disengage **Choose automatically** and add a new server to the **Update server** field using one of the following formats:
  http://IP_address_of_your_server:2221
  https://IP_address_of_your_server:2221 (if SSL is used)

Accessing the Mirror via system shares

First, a shared folder should be created on a local or network device. When creating the folder for the Mirror, you must provide *"write"* access for the user who will save update files to the folder and *"read"* access for all users who will update ESET Mail Security from the Mirror folder.

Next, configure access to the Mirror in **Advanced setup** > **Update**> **Mirror** tab by disabling **Provide update files via internal HTTP server**. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must enter authentication data to access the other computer. To enter authentication data, open ESET Mail Security **Advanced setup** (F5) and click **Update** > **Connect to LAN as**. This is the same setting used for updating, as described in the Connect to LAN as section.

After Mirror configuration is complete, on client workstations set *UNC**PATH* as the update server using the steps below:

1. Open ESET Mail Security **Advanced setup** and click **Update** > **Basic**.
2. Click **Update server** and add a new server using the *UNC**PATH* format.

NOTE: For updates to function properly, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

The last section controls program components (PCUs). By default, downloaded program components are prepared to copy to the local mirror. If **Program component update** is activated, there is no need to click **Update**, because files are copied to the local mirror automatically when they are available. See Update mode for more information about program component updates.

5.3.5.2 Mirror files

List of available and localized program component files.

5.3.5.3 Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data for the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

- **ESET Mail Security reports an error connecting to Mirror server** - Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, enter the folder name and click **OK**. The contents of the folder should be displayed.
- **ESET Mail Security requires a username and password** - Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, *Domain/Username*, or *Workgroup/Username*, plus the corresponding Passwords. If the Mirror server is accessible to "Everyone", please be aware that this does not mean that any user is granted access. "Everyone" does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to "Everyone", a domain username and password will still need to be entered in the update setup section.
- **ESET Mail Security reports an error connecting to the Mirror server** - Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

5.3.6 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking **Update** from the main menu.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Mail Security:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see the Scheduler section of this guide.

5.4 Web and email

The **Web and email** section allows you to configure Email client protection, protect your Internet communication using the Web access protection and control the Internet protocols by configuring the Protocol filtering. These features are vital for protecting your computer when communicating through the Internet.

The **Email client protection** controls all email communication, protects against malicious code and lets you choose the action taken when an infection is detected.

Web access protection monitors the communication between web browsers and remote servers and complies with the HTTP and HTTPS rules. This feature also allows you to block, allow or exclude certain URL addresses.

The **Protocol filtering** is an advanced protection for the application protocols and it is provided by the ThreatSense scanning engine. This control works automatically, whether a web browser or an email client is used. It also works for the encrypted (SSL/TLS) communication.

NOTE: On Windows Server 2008 and Windows Server 2008 R2, installation of **Web and email** component is disabled by default. If you want this feature to be installed, choose **Custom** installation type. If you have ESET Mail Security already installed, you can run the installer again to modify your existing installation adding Web and email component.

5.4.1 Protocol filtering

Protocol filtering

Antivirus protection for application protocols is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. To edit encrypted (SSL) settings, go to **Web and email** > **SSL/TLS**.

Enable application protocol content filtering - Can be used to disable protocol filtering. Note that many ESET Mail Security components (Web access protection, Email protocols protection and Anti-Phishing) depend on this and will be non-functional without it.

Excluded applications - Allows you to exclude specific remote addresses from protocol filtering. Useful when protocol filtering causes compatibility issues.

Excluded IP addresses - Allows you to exclude specific applications from protocol filtering. Useful when protocol filtering causes compatibility issues.

Web and email clients - Used only on Windows operating systems, allows you to select applications for which all traffic is filtered by protocol filtering, regardless of ports used.

Record information necessary for ESET support to diagnose protocol filtering issues - Enables advanced logging of diagnostics data, use this only when requested to by ESET support.

5.4.1.1 Excluded applications

To exclude the communication of specific network-aware applications from content filtering, select them in the list. HTTP/POP3 communication of the selected applications will not be checked for threats. We recommend using this option only for applications that do not work properly with their communication being checked.

Applications and services that were already affected by protocol filtering will be automatically displayed after clicking **Add**.

Edit - Edit selected entries from the list.
Remove - Remove selected entries from the list.

5.4.1.2 Excluded IP addresses

IP addresses in this list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Add - Click to add an IP address/address range/subnet of a remote point to which a rule is applied.

Edit - Edit selected entries from the list.

Remove - Remove selected entries from the list.

5.4.1.3 Web and email clients

NOTE: Starting with Windows Vista Service Pack 1 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since WFP technology uses special monitoring techniques, the **Web and email clients** section is not available.

Because of the enormous amount of malicious code circulating the Internet, safe Internet browsing is a very important aspect of computer protection. Web browser vulnerabilities and fraudulent links help malicious code enter the system unnoticed, which is why ESET Mail Security focuses on web browser security. Each application accessing the network can be marked as an Internet browser. Applications that already use protocols for communication or applications from selected paths can be added to the list of Web and email clients.

5.4.2 SSL/TLS

ESET Mail Security is capable of checking for threats in communications that use the SSL/TLS protocol. You can use various scanning modes to examine SSL protected communications with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering - If protocol filtering is disabled, the program will not scan communications over SSL/TLS.

SSL/TLS protocol filtering mode is available in following options:

- **Automatic mode** - Select this option to scan all SSL/TLS protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.
- **Interactive mode** - If you enter a new SSL/TLS protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL/TLS certificates that will be excluded from scanning.

Block encrypted communication utilizing the obsolete protocol SSL v2 - Communication using the earlier version of the SSL protocol will automatically be blocked.

Root certificate

Root certificate - For SSL/TLS communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). **Add the root certificate to known browsers** should be enabled. Select this option to automatically add the ESET root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and manually import it into the browser.

Certificate validity

If the certificate cannot be verified using the TRCA certificate store - In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store. This means that the certificate is signed by someone (for example, the administrator of a web server or a small business) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by the TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. You can select **Block communication that uses the certificate** to always terminate encrypted connections to sites with unverified certificates.

If the certificate is invalid or corrupt - This means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave **Block communication that uses the certificate** selected.

List of known certificates allows you to customize ESET Mail Security behavior for specific SSL certificates.

5.4.2.1 Encrypted SSL communication

If your system is configured to use SSL protocol scanning, a dialog window prompting you to choose an action will be displayed in two situations:

First, if a website uses an unverifiable or invalid certificate, and ESET Mail Security is configured to ask the user in such cases (by default yes for unverifiable certificates, no for invalid ones), a dialog box will ask you whether to **Allow** or **Block** the connection.

Second, if **SSL protocol filtering mode** is set to **Interactive mode**, a dialog box for each website will ask whether to **Scan** or **Ignore** the traffic. Some applications verify that their SSL traffic is not modified nor inspected by anyone, in such cases ESET Mail Security must **Ignore** that traffic to keep the application working.

In both cases, the user can choose to remember the selected action. Saved actions are stored in the **List of known certificates**.

5.4.2.2 List of known certificates

The **List of known certificates** can be used to customize ESET Mail Security behavior for specific SSL certificates, and to remember actions chosen if **Interactive mode** is selected in **SSL protocol filtering mode**. The list can be viewed and edited in **Advanced setup** (F5) > **Web and email** > **SSL protocol checking** > **List of known certificates**.

The **List of known certificates** window consists of:

Columns

- **Name** - Name of the certificate.
- **Certificate issuer** - Name of the certificate creator.
- **Certificate subject** - The subject field identifies the entity associated with the public key stored in the subject public key field.
- **Access** - Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to always ask user what to do.
- **Scan** - Select **Scan** or **Ignore** as the **Scan action** to scan or ignore communication secured by this certificate. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

- **Edit** - Select the certificate that you want to configure and click **Edit**.
- **Remove** - Select the certificate that you want to delete and click **Remove**.
- **OK/Cancel** - Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

5.4.3 Email client protection

Integration of ESET Mail Security with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET Mail Security. When integration is activated, the ESET Mail Security toolbar is inserted directly into the email client (toolbar for newer versions of Windows Live Mail is not inserted), allowing for more efficient email protection. Integration settings are located under **Setup** > **Advanced setup** > **Web and email** > **Email client protection** > **Email clients**.

Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

Turn on **Disable checking upon inbox content change** if you are experiencing a system slowdown when working with your email client (MS Outlook only). This can occur when retrieving email from the Kerio Outlook Connector Store.

Email to scan

Received email - Toggles checking of received messages.
Sent email - Toggles checking of sent messages.
Read email - Toggles checking of read messages.

Action to be performed on infected email

No action - If enabled, the program will identify infected attachments, but will leave emails without taking any action.
Delete email - The program will notify the user about infiltration(s) and delete the message.
Move email to the Deleted items folder - Infected emails will be moved automatically to the Deleted items folder.
Move email to the folder - Infected emails will be moved automatically to the specified folder.

Folder - Specify the custom folder where you want to move infected emails when detected.

Repeat scan after update - Toggles rescanning after a virus signature database update.

Accept scan results from other modules - If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

5.4.3.1 Email protocols

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. ESET Mail Security provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client.

You can configure IMAP/IMAPS and POP3/POP3S protocol checking in Advanced setup. To access this setting, expand **Web and email** > **Email client protection** > **Email protocols**.

ESET Mail Security also supports the scanning of IMAPS and POP3S protocols, which use an encrypted channel to transfer information between server and client. ESET Mail Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by IMAPS/POP3S protocol**, regardless of operating system version.

Encrypted communications will be not scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL/TLS protocol checking in Advanced setup, click **Web and email** > **SSL/TLS** and select **Enable SSL/TLS protocol filtering**.

5.4.3.2 Alerts and notifications

Email protection provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other e-mail clients, ESET Mail Security provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.

The options for this functionality are available in **Advanced setup** under **Web and email** > **Email client protection** > **Alerts and notifications**.

ThreatSense parameters - The advanced virus scanner setup enables you to configure scan targets, detection methods, etc. Click to display the detailed virus scanner setup window.

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read mail, Append note to the subject of received and read infected email** or **Append tag messages to sent email**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The available options are:

- **Never** - No tag messages will be added at all.
- **To infected email only** - Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** - The program will append messages to all scanned email.

Append note to the subject of sent infected email - Disable this if you do not want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient and if an

infiltration is detected, provides valuable information about the threat level of a given email or sender.

Template added to the subject of infected email - Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject *"Hello"* with a given prefix value *"[virus]"* to the following format: *"[virus] Hello"*. The variable *%VIRUSNAME%* represents the detected threat.

5.4.3.3 MS Outlook toolbar

Microsoft Outlook protection works as a plug-in module. After ESET Mail Security is installed, this toolbar containing the antivirus protection options is added to Microsoft Outlook:

ESET Mail Security - Click on icon opens the main program window of ESET Mail Security.

Rescan messages - Enables you to launch email checking manually. You can specify messages that will be checked and you can activate rescanning of received email. For more information see Email client protection.

Scanner setup - Displays the Email client protection setup options.

5.4.3.4 Outlook Express and Windows Mail toolbar

Outlook Express and Windows Mail protection works as a plug-in module. After ESET Mail Security is installed, this toolbar containing the antivirus protection options is added to Outlook Express or Windows Mail:

ESET Mail Security - Click on icon opens the main program window of ESET Mail Security.

Rescan messages - Enables you to launch email checking manually. You can specify messages that will be checked and you can activate rescanning of received email. For more information see Email client protection.

Scanner setup - Displays the Email client protection setup options.

User interface

Customize appearance - The appearance of the toolbar can be modified for your email client. Deselect the option to customize appearance independent of email program parameters.

Show text - Displays descriptions for icons.

Text to the right - Option descriptions are moved from the bottom to the right side of icons.

Large icons - Displays large icons for menu options.

5.4.3.5 Confirmation dialog

This notification serves to verify that user really wants to perform the selected action, which should eliminate possible mistakes.

On the other hand, the dialog also offers the option to disable confirmations.

5.4.3.6 Rescan messages

The ESET Mail Security toolbar integrated in email clients enables users to specify several options for email checking. The option **Rescan messages** offers two scanning modes:

All messages in the current folder - Scans messages in the currently displayed folder.

Selected messages only - Scans only messages marked by the user.

The **Rescan already scanned messages** check box provides the user with the option to run another scan on messages that have been scanned before.

5.4.4 Web access protection

Internet connectivity is a standard feature on most personal computers. Unfortunately, it has also become the main medium for transferring malicious code. Web access protection works by monitoring communication between web browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules.

Access to web pages known to contain malicious content is blocked before content is downloaded. All other webpages are scanned by the ThreatSense scanning engine when they are loaded and blocked if malicious content is detected. Web access protection offers two level of protection, blocking by blacklist and blocking by content.

We strongly recommend that you leave Web access protection enabled. This option can be accessed from the main program window of ESET Mail Security by navigating to **Setup** > **Computer** > **Web access protection**.

The following options are available in **Advanced setup** (F5) > **Web and email** > **Web access protection**:

- **Basic** - lets you enable or disable whole Web access protection. When disabled, options below will become inactive.
- **Web protocols** - enables you to configure monitoring for these standard protocols which are used by most Internet browsers.
- **URL address management** - enables you to specify HTTP addresses to block, allow or exclude from checking.
- **ThreatSense engine parameter setup** - Advanced virus scanner setup - enables you to configure settings such as types of objects to scan (emails, archives, etc.), detection methods for Web access protection etc.

Web protocols

By default, ESET Mail Security is configured to monitor the HTTP protocol used by most Internet browsers.

In Windows Vista and later, HTTP traffic is always monitored on all ports for all applications. In Windows XP/2003, you can modify the **Ports used by HTTP protocol** in **Advanced setup** (F5) > **Web and email** > **Web access protection** > **Web protocols** > **HTTP scanner setup**. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

ESET Mail Security also supports HTTPS protocol checking. HTTPS communication uses an encrypted channel to transfer information between server and client. ESET Mail Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version.

Encrypted communication will be not scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL protocol checking in Advanced setup, click **Web and email** > **SSL protocol checking** and select **Enable SSL protocol filtering**.

5.4.4.1 Basic

Choose whether you want to have **Web access protection** enabled (default) or disabled. When disabled, options below will become inactive.

NOTE: We strongly recommend that you leave Web access protection enabled. This option can also be accessed from the main program window of ESET Mail Security by navigating to **Setup** > **Computer** > **Web access protection**.

5.4.4.2 URL address management

The URL address management section allows you to specify HTTP addresses to block, allow or exclude from checking.

Websites in the **List of blocked addresses** will not be accessible unless they are also included in the **List of allowed addresses**. Websites in the **List of addresses excluded from checking** are not scanned for malicious code when accessed.

Enable SSL/TLS protocol filtering must be selected if you want to filter HTTPS addresses in addition to HTTP web pages. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk represents any number or character, while the question mark represents any one character. Particular care should be taken when specifying excluded addresses because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

If you want to block all HTTP addresses except addresses present in the active **List of allowed addresses**, add * to the active **List of blocked addresses.**

Add - Creates a new list in addition to the predefined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from some external public blacklist, and a second one may contain your own blacklist, which makes it easier to update the external list while keeping yours intact.
Edit - Modifies existing lists. Use this to add or remove addresses from the lists.
Remove - Deletes existing list. Only possible for lists created with **Add**, not for the default ones.

5.4.4.2.1 Create new list

This section allows you to specify lists of URL addresses/masks that will be blocked, allowed or excluded from checking.

When creating a new list, the following options are available to configure:

Address list type - Three list types are available:

- **List of addresses excluded from checking** - No checking for malicious code will be performed for any address added to this list.
- **List of blocked addresses** - The user will not be allowed to access addresses specified in this list. This applies only to HTTP protocol. Other protocols than HTTP will not be blocked.
- **List of allowed addresses** - If the Allow access only to HTTP addresses in the list of allowed addresses option is enabled and the list of blocked addresses contain * (match everything), user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they also match by the list of blocked addresses.

List name - Specify the name of the list. This field will be grayed out when editing one of the three predefined lists.

List description - Type a short description for the list (optional). Will be grayed when editing one of three predefined list.

To activate a list, select **List active** next to that list. If you want to be notified when a particular list is used in evaluation of an HTTP site that you visited, select **Notify when applying**. For example, a notification will be issued if a website is blocked or allowed because it is included in list of blocked or allowed addresses. The notification will contain the name of the list containing the specified website.

Add - Add a new URL address to the list (enter multiple values with separator).

Edit - Modifies existing address in the list. Only possible for addresses created with **Add**.

Remove - Deletes existing addresses in the list. Only possible for addresses created with **Add**.

Import - Import a file with URL addresses (separate values with a line break, for example *.txt using encoding UTF-8).

5.4.4.2.2 Address list

In this section you can specify lists of HTTP addresses that will be blocked, allowed or excluded from checking.

By default, the following three lists are available:

- **List of addresses excluded from checking** - No checking for malicious code will be performed for any address added to this list.
- **List of allowed addresses** - If **Allow access only to HTTP addresses in the list of allowed addresses** is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they are included in the list of blocked addresses.
- **List of blocked addresses** - The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.

Click **Add** to create a new list. To delete selected lists, click **Remove**.

5.4.5 Anti-Phishing protection

ESET Mail Security also provides protection against phishing. Anti-Phishing protection is part of Web and email module. If you have installed ESET Mail Security using **Complete** installation type, Web and email is installed by default with Anti-Phishing protection enabled. However, this does not apply to systems running Microsoft Windows Server 2008.

NOTE: Web and email component is not part of **Complete** ESET Mail Security installation type on Windows Server 2008 or Windows Server 2008 R2 system. If required, you can modify existing installation adding Web and email component in order to be able to use Anti-Phishing protection.

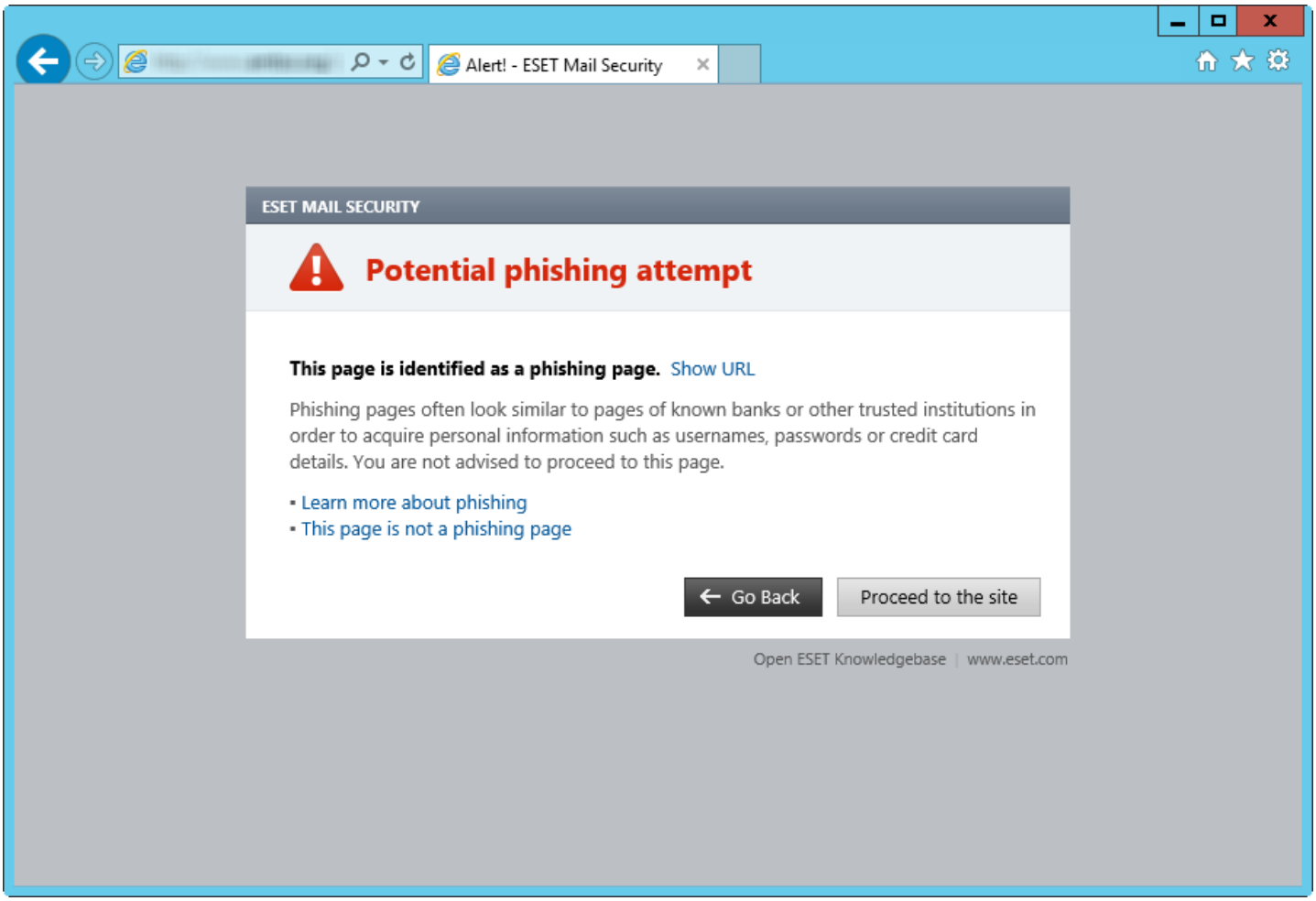
The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET Mail Security includes anti-phishing protection, which blocks web pages known to distribute this type of content.

We strongly recommend that you enable Anti-Phishing in ESET Mail Security. To do so, open **Advanced setup** (F5) and navigate to **Web and email** > **Anti-Phishing protection**.

Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET Mail Security.

Accessing a phishing website

When you access a recognized phishing website, the following dialog will be displayed in your web browser. If you still want to access the website, click **Proceed to the site** (not recommended).


Alert! - ESET Mail Security
ESET MAIL SECURITY
Potential phishing attempt
This page is identified as a phishing page. Show URL
Phishing pages often look similar to pages of known banks or other trusted institutions in order to acquire personal information such as usernames, passwords or credit card details. You are not advised to proceed to this page.
Learn more about phishing
This page is not a phishing page
Go Back
Proceed to the site
Open ESET Knowledgebase | www.eset.com

NOTE: Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool. From **Advanced setup** (F5) expand **Web and email** > **Web access protection** > **URL address management** > **Address list**, click **Edit** and then add the website that you want to edit to the list.

Phishing site reporting

The Report link enables you to report a phishing/malicious website to ESET for analysis.

NOTE: Before submitting a website to ESET, make sure it meets one or more of the following criteria:

- the website is not detected at all
- the website is incorrectly detected as a threat. In this case, you can Report a false-positive phishing site.

Alternatively, you can submit the website by email. Send your email to samples@eset.com. Remember to use a descriptive subject and enclose as much information about the website as possible (for example, the website that referred you there, how you learned of this website, etc.).

5.5 Device control

ESET Mail Security provides automatic device (CD/DVD/USB/) control. This module allows you to scan, block or adjust extended filters/permissions and define a users ability to access and work with a given device. This may be useful if the computer administrator wants to prevent the use of devices containing unsolicited content.

Supported external devices:

- Disk storage (HDD, USB removable disk)
- CD/DVD
- USB printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device
- All device types

Device control setup options can be modified in **Advanced setup** (F5) > **Device control**.

Enabling the switch next to **Integrate into system** activates the Device control feature in ESET Mail Security; you will need to restart your computer for this change to take effect. Once Device control is enabled, **Rules editor** will become active, allowing you to open the Rules editor window.

If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device will not be granted.

5.5.1 Device control - Rules editor

The **Device control rules editor** window displays existing rules and allows for precise control of external devices that users connect to the computer.

Specific devices can be allowed or blocked by user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as its name, the type of external device, the action to perform after connecting an external device to your computer, and log severity.

Click **Add** or **Edit** to manage a rule. Click **Remove** if you want to delete the selected rule or deselect the **Enabled** check box next to a given rule to disable it. This can be useful if you don't want to delete a rule permanently so that you can use it in the future.

Copy - Creates a new rule based on the parameters of the selected rule.

Click **Populate** to auto-populate removable media device parameters for devices connected to your computer.

Rules are listed in order of priority with higher-priority rules closer to the top. You can select multiple rules and apply actions, such as deleting or moving them up or down the list by clicking the **Top/Up/Down/Bottom** (arrow buttons).

Log entries can be viewed from the main program window of ESET Mail Security in **Tools** > Log files.

5.5.2 Adding Device control rules

A Device control rule defines the action that will be taken when a device meeting the rule criteria is connected to the computer.

Enter a description of the rule into the **Name** field for better identification. Click the switch next to **Rule enabled** to disable or enable this rule; this can be useful if you don't want to delete the rule permanently.

Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). The types of devices are inherited from the operating system and can be seen in the system Device manager assuming the device is connected to the computer. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Smart card readers include all readers of smart cards with an embedded integrated circuit, such as SIM cards or authentication cards. Examples of imaging devices are scanners or cameras, these devices do not provide information about users, only about their actions. This means that imaging devices can only be blocked globally.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices allow you to select one of the following rights settings:

- **Read/Write** - Full access to the device will be allowed.
- **Block** - Access to the device will be blocked.
- **Read Only** - Only read access to the device will be allowed.
- **Warn** - Each time that a device is connected, the user will be notified if it is allowed/blocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed upon subsequent connections of the same device.

Please note that not all rights (actions) are available for all device types. If a device has storage space, all four actions are made available. For non-storage devices, there are only two (for example **Read Only** is not available for Bluetooth , so Bluetooth devices can only be allowed or blocked).

Additional parameters shown below can be used to fine-tune rules and tailor them to devices. All parameters are case-insensitive:

- **Vendor** - Filter by vendor name or ID.
- **Model** - The given name of the device.
- **Serial** - External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

NOTE: If these three descriptors are empty, the rule will ignore these fields when matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

Tip: In order to figure out the parameters of a device, create a rule to allow that type of device, connect the device to your computer and then review the device details in the Device control log.

Severity

- **Always** - Logs all events.
- **Diagnostic** - Logs information needed to fine-tune the program.
- **Information** - Records informative messages, including successful update messages, plus all records above.
- **Warning** - Records critical errors and warning messages.
- **None** - No logs will be recorded.

Rules can be limited to certain users or user groups by adding them to the **User list**:

- **Add** - Opens the **Object types: Users or Groups** dialog window that allows you to select desired users.
- **Remove** - Removes the selected user from the filter.

NOTE: All devices can be filtered by user rules (for example imaging devices do not provide information about

users, only about invoked actions).

5.5.3 Detected devices

The **Populate** button provides an overview of all currently connected devices with the following information: device type, device vendor, model and serial number (if available). When you select a device (from the list of Detected devices) and click **OK**, a rule editor window appears with predefined information (you can adjust all the settings).

5.5.4 Device groups

Device connected to your computer may pose a security risk.

The Device groups window is divided into two parts. The right part of the window contains a list of devices that belong to a respective group and the left part of the window contains a list of existing groups. Select the group that contains the devices you want to display in the right pane.

When you open the Device groups window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file. Alternatively, you can click **Populate** and all devices connected to your computer will be listed in the **Detected devices** window. Select a device from the populated list to add it to the group by clicking **OK**.

Control elements

Add - You can add a group by entering its name, or add a device to an existing group. (optionally, you can specify details such as vendor name, model and serial number) depending on where in the window you clicked the button.

Edit - Lets you modify the name of a selected group or parameters for the devices contained therein (vendor, model, serial number).

Remove - Deletes the selected group or device depending on where in the window you clicked.

Import - Imports a list of devices from a file.

The **Populate** button provides an overview of all currently connected devices with the following information: device type, device vendor, model and serial number (if available).

When you are done with customization click **OK**. Click **Cancel** if you want to leave the **Device groups** window without saving changes.

TIP: You can create different groups of devices for which different rules will be applied. You can also create only one group of devices for which the rule with action **Read/Write** or **Read only** will be applied. This ensures that unrecognized devices will be blocked by Device control when connected to your computer.

Note that not all Actions (permissions) are available for all device types. For storage devices, all four Actions are available. For non-storage devices, there are only three Actions available (for example **Read Only** is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).

5.6 Tools

The following are advanced settings for all the tools ESET Mail Security offers under **Tools** tab in the main GUI window.

5.6.1 ESET LiveGrid

ESET LiveGrid is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting. New threat information is streamed in real-time to the cloud, which enables the ESET Malware Research Lab to provide timely response and consistent protection at all times. Users can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid. When installing ESET Mail Security, select one of the following options:

1. You can decide not to enable ESET LiveGrid. Your software will not lose any functionality, but in some cases ESET Mail Security may respond slower to new threats than virus signature database update.
2. You can configure ESET LiveGrid to submit anonymous information about new threats and where the new threatening code was detected. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

ESET LiveGrid will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer‘s operating system.

By default, ESET Mail Security is configured to submit suspicious files for detailed analysis to the ESET Virus Lab. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are particular files that you or your organization want to avoid sending.

The ESET LiveGrid reputation system provides cloud-based whitelisting and blacklisting. To access settings for ESET LiveGrid, press **F5** to enter Advanced setup and expand **Tools** > **ESET LiveGrid**.

Enable ESET LiveGrid reputation system (recommended) - The ESET LiveGrid reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

Submit anonymous statistics - Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, product version, and configuration including information about your system.

Submit files - Suspicious files resembling threats, and/or files with unusual characteristics or behavior are submitted to ESET for analysis.

Select **Enable logging** to create an event log to record file and statistical information submissions. This will enable logging to the Event log when files or statistics are sent.

Contact email (optional) - Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

Exclusions - The Exclusion filter allows you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

If you have used ESET LiveGrid before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. Once all current information is sent, no further packages will be created.

5.6.1.1 Exclusion filter

The **Edit** option next to Exclusions in ESET LiveGrid allows you to configure how threats are submitted to ESET Virus Labs for analysis.

If you find a suspicious file, you can submit it for analysis to our ThreatLabs. If it is a malicious application, its detection will be added to the next virus signature update.

5.6.2 Quarantine

Infected or suspicious files are stored in a benign form in the quarantine folder. The real-time protection module quarantines all newly created suspicious files by default to avoid infection.

Rescan quarantined files after every update - All quarantined objects will be scanned after each virus signature database update. This is especially useful if a file has been moved to quarantine as a result of false positive detection. With this option enabled, certain types of files can automatically be restored to their original location.

5.6.3 Microsoft Windows update

Windows updates provide important fixes to potentially dangerous vulnerabilities and improve the general security level of your computer. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET Mail Security notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** - No system updates will be offered for download.
- **Optional updates** - Updates marked as low priority and higher will be offered for download.
- **Recommended updates** - Updates marked as common and higher will be offered for download.
- **Important updates** - Updates marked as important and higher will be offered for download.
- **Critical updates** - Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Sytem update information may not be immediately available after saving changes.

5.6.4 WMI Provider

About WMI

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

For more information on WMI, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

The purpose of the ESET WMI Provider is to allow for the remote monitoring of ESET products in an enterprise environment without requiring any ESET-specific software or tools. By exposing the basic product, status and statistics information via WMI, we greatly expand the possibilities of enterprise administrators when monitoring the ESET products. Administrators can take advantage of the number of access methods offered by WMI (command line, scripts and third-party enterprise monitoring tools) to monitor the state of their ESET products.

The current implementation provides read-only access to basic product information, installed features and their protection status, statistics of individual scanners, and product log files.

The WMI Provider allows for the use of standard Windows WMI infrastructure and tools to read the state of the product and product logs.

5.6.4.1 Provided data

All the WMI classes related to ESET product are located in the “root\ESET“ namespace. The following classes, which are described in more detail below, are currently implemented:

General:

- ESET_Product
- ESET_Features
- ESET_Statistics

Logs:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

ESET_Product class

There can be only one instance of the ESET_Product class. Properties of this class refer to basic information about your installed ESET product:

- **ID** - product type identifier, for example, “essbe”
- **Name** - name of the product, for example, "ESET Security"
- **Edition** - edition of the product, for example, "Microsoft SharePoint Server"
- **Version** - Product version, for example, "4.5.15013.0"
- **VirusDBVersion** - version of the virus database, for example, "7868 (20130107)"
- **VirusDBLastUpdate** - timestamp of the last update of the virus database. The string contains the timestamp in WMI datetime format. for example, “20130118115511.000000+060”
- **LicenseExpiration** - license expiration time. The string contains timestamp in WMI datetime format. for example, “20130118115511.000000+060”
- **KernelRunning** - boolean value indicating whether the eKrn service is running on the machine, for example, “TRUE”
- **StatusCode** - number indicating the protection status of the product: 0 - Green (OK), 1 - Yellow (Warning), 2 - Red (Error)
- **StatusText** - message describing the reason for a non-zero status code, otherwise it is null

ESET_Features class

The ESET_Features class has multiple instances, depending on the number of product features. Each instance contains:

- **Name** - name of the feature (list of names is provided below)
- **Status** - status of the feature: 0 - inactive, 1 - disabled, 2 - enabled

A list of strings representing currently recognized product features:

- **CLIENT_FILE_AV** - real-time file system anti-virus protection
- **CLIENT_WEB_AV** - client web anti-virus protection
- **CLIENT_DOC_AV** - client document anti-virus protection
- **CLIENT_NET_FW** - client personal firewall
- **CLIENT_EMAIL_AV** - client email anti-virus protection
- **CLIENT_EMAIL_AS** - client email anti-spam protection
- **SERVER_FILE_AV** - real-time anti-virus protection of files on the protected file server product, for example, files in SharePoint's content database in the case of ESET Mail Security
- **SERVER_EMAIL_AV** - anti-virus protection of emails of protected server product, for example, emails in MS Exchange or IBM Domino
- **SERVER_EMAIL_AS** - anti-spam protection of emails of protected server product, for example, emails in MS Exchange or IBM Domino
- **SERVER_GATEWAY_AV** - anti-virus protection of protected network protocols on the gateway
- **SERVER_GATEWAY_AS** - anti-spam protection of protected network protocols on the gateway

ESET_Statistics class

The ESET_Statistics class has multiple instances, depending on the number of scanners in the product. Each instance contains:

- Scanner - string code for the particular scanner, for example, "CLIENT_FILE"
- Total - total number of files scanned
- Infected - number of infected files found
- Cleaned - number of cleaned files
- Timestamp - timestamp of the last change of this statistics. In WMI datetime format, for example, "20130118115511.000000+060"
- ResetTime - timestamp of when the statistics counter was last reset. In WMI datetime format, for example, "20130118115511.000000+060"

List of strings representing currently recognized scanners:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

ESET_ThreatLog class

The ESET_ThreatLog class has multiple instances, each one representing a log record from the "Detected threats" log. Each instance contains:

- **ID** - unique ID of this log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number in the [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner** - Name of the scanner that created this log event
- **ObjectType** - Type of object that produced this log event
- **ObjectName** - Name of the object that produced this log event
- **Threat** - Name of the threat that has been found in the object described by ObjectName and ObjectType properties
- **Action** - Action performed after the threat was identified
- **User** - User account that caused this log event to be generated
- **Information** - Additional description of the event

ESET_EventLog

The ESET_EventLog class has multiple instances, each one representing a log record from the “Events” log. Each instance contains:

- **ID** - unique ID of this log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module** - Name of the module that created this log event
- **Event** - Description of the event
- **User** - User account that caused this log event to be generated

ESET_ODFileScanLogs

The ESET_ODFileScanLogs class has multiple instances, each one representing an on-demand file scan record. This is equivalent to the GUI “On-demand computer scan” list of logs. Each instance contains:

- **ID** - unique ID of this on-demand log
- **Timestamp** - creation timestamp of the log (in the WMI date/time format)
- **Targets** - Target folders/objects of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **Status** - Status of the scan process

ESET_ODFileScanLogRecords

The ESET_ODFileScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODFileScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ODFileScanLogs class)
- **ID** - unique ID of this scan log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

ESET_ODServerScanLogs

The ESET_ODServerScanLogs class has multiple instances, each one representing a run of the on-demand server scan. Each instance contains:

- **ID** - unique ID of this on-demand log
- **Timestamp** - creation timestamp of the log (in the WMI date/time format)
- **Targets** - Target folders/objects of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **RuleHits** - Total number of rule hits
- **Status** - Status of the scan process

ESET_ODServerScanLogRecords

The ESET_ODServerScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODServerScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ ODServerScanLogs class)
- **ID** - unique ID of this scan log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

ESET_GreylistLog

The ESET_GreylistLog class has multiple instances, each one representing a log record from the “Greylist” log. Each instance contains:

- **ID** - unique ID of this log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain** - Name of the HELO domain
- **IP** - Source IP address
- **Sender** - Email sender
- **Recipient** - Email recipient
- **Action** - Action performed
- **TimeToAccept** - Number of minutes after which the email will be accepted

ESET_SpamLog

The ESET_SpamLog class has multiple instances, each one representing a log record from the “Spamlog”. Each instance contains:

- **ID** - unique ID of this log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sender** - Email sender
- **Recipients** - Email recipients
- **Subject** - Email subject
- **Received** - Time of reception
- **Score** - Spam score in percent [0-100]
- **Reason** - The reason this email was marked as spam
- **Action** - Action performed
- **DiagInfo** - Additional diagnostic information

5.6.4.2 Accessing Provided Data

Here are a few examples of how to access ESET WMI data from Windows command line and PowerShell, which should work from any current Windows operating system. There are, however, many other ways of accessing the data from other scripting languages and tools.

Command line without scripts

The `wmic` command line tool can be used to access various predefined or any custom WMI classes.

To display complete info about product on the local machine:
```
wmic /namespace:\\root\ESET Path ESET_Product
```

To display product version number only of the product on the local machine:
```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

To display complete info about product on a remote machine with IP 10.1.118.180:
```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Get and display complete info about product on the local machine:
```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Get and display complete info about product on a remote machine with IP 10.1.118.180:
```
$cred = Get-Credential            # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

5.6.5 ERA scan targets

This functionality lets ESET Remote Administrator to use appropriate On-demand database scan targets when running **Server Scan** Client task on a server with ESET Mail Security.

When you enable **Generate target list** functionality, ESET Mail Security creates a list of currently available database scan targets. This list is generated periodically, according to defined **Update period** in minutes. When ERA wants to run **Server Scan** Client task, it will collect the list and lets you choose scan targets for On-demand database scan on that particular server.

5.6.6 Log files

This section let's you modify configuration of ESET Mail Security logging. You can use the switches to disable or enable particular feature. To start the actual logging you need to turn on general diagnostic logging on product level in main menu > **Setup** > Tools. Once the logging itself is turned on, ESET Mail Security will collect detailed logs according to what features are enabled in this section. All records are written to the **Events** log (`C:\ProgramData\ESET\ESET Mail Security\Logs\warnlog.dat`) and can be viewed in Log files viewer.

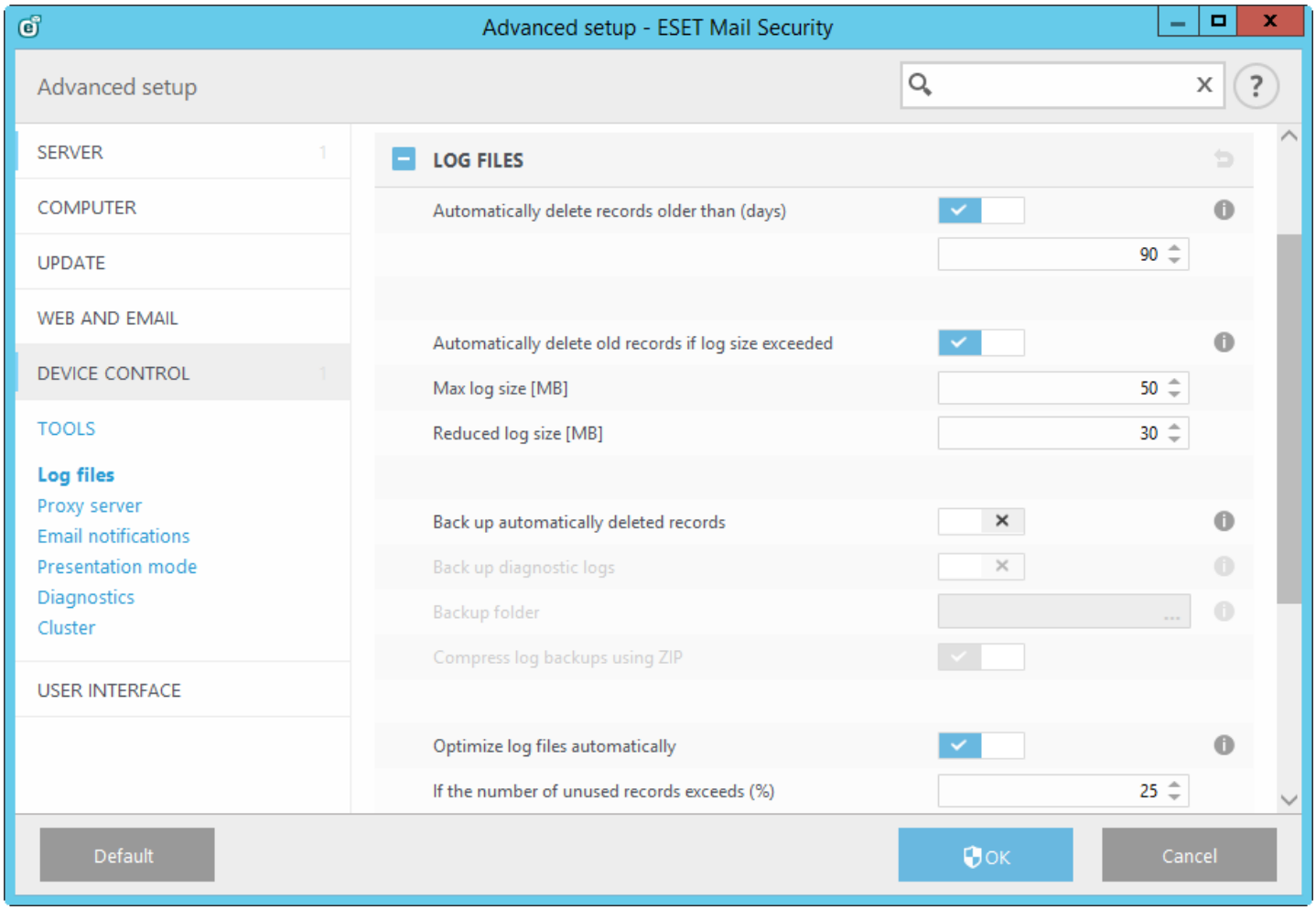
Log records

Log mail transport errors - if this option is enabled and should there be problems on the mail transport layer, error messages are written into Events log.
Log mail transport exceptions - if there are any exception on the mail transport layer, details about it are written into Events log.

Diagnostic logging

Database protection diagnostic logging
Mail transport diagnostic logging
On-demand database scan diagnostic logging
Cluster diagnostic logging - you can use switch to disable or enable **Cluster Diagnostic logging** if required. It is enabled by default. This means that Cluster logging will be included in general diagnostic logging.

Log files - you can define how the logs will be managed. The program automatically deletes older logs in order to save disk space.



Log entries older than the specified number of days in the **Automatically delete records older than (days)** field will automatically be deleted.
Automatically delete old records if log size exceeded - when log size exceeds **Max log size [MB]**, old log records will be deleted until **Reduced log size [MB]** is reached.

Back up automatically deleted records - automatically deleted log records and files will be backed up to the specified directory and optionally compressed as ZIP files
Back up diagnostic logs - will back up automatically deleted diagnostic logs. If not enabled, diagnostic log records are not backed up.
Backup folder - folder where log backups will be stored. You can enable **compressed log backups using ZIP**.

Optimize log files automatically - When engaged, log files will automatically be defragmented, if fragmentation percentage is higher than value specified in the **If the number of unused records exceeds (%)** field.

Click **Optimize log files** to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed especially if the logs contain a large number of entries.

Turn on **Enable text protocol** to enable the storage of logs in another file format separate from Log files:

- **Target directory** - The directory where log files will be stored (only applies to Text/CSV). Each log section has its own file with a predefined file name (for example, *virlog.txt* for **Detected threats** section of Log files, if you use plain text file format to store logs).
- **Type** - If you select the **Text** file format, logs will be stored in a text file; data will be separated by tabs. The same applies to comma-separated **CSV** file format. If you choose **Event**, logs will be stored in the Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to file.

Delete all log files - erases all stored logs currently selected in the **Type** drop-down menu.

5.6.6.1 Log filtering

Logs store information about important system events. The log filtering feature allows you to display records about a specific type of event.

Enter the search keyword into the **Find text** field. Use the **Search in columns** drop-down menu to refine your search.

Record types - Choose one or more record log types from the drop-down menu:

- **Diagnostic** - Logs information needed to fine-tune the program and all records above.
- **Informative** - Records informative messages, including successful update messages, plus all records above.
- **Warnings** - Records critical errors and warning messages.
- **Errors** - Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** - Logs only critical errors (error starting antivirus protection).

Time period - Define the time period from which you want the results to be displayed.

Match whole words only - Select this check box if you want to search for specific whole words for more precise results.

Case sensitive - Enable this option if it is important for you to use capital or lower case letters while filtering.

5.6.6.2 Find in log

In addition to Log filtering, you can use the search functionality within Log files, however you can also use it independently from log filtering. This is useful when you are looking for particular records in logs. Like Log filtering, this search feature will help you find the information you are looking for, especially when there are too many records.

When using search in log, you can **Find text** by typing a specific string, use the **Search in columns** drop-down menu to filter by column, select **Record types** and set a **Time period** to only search for records from a specific time period. By specifying certain search options, only records that are relevant (according to those search options) will be searched in the Log files window.

Find text: Type a string (word, or part of a word). Only records that contain this string will be found. Other records will be omitted.

Search in columns: Select what columns will be taken into account when searching. You can check one or more columns to be used for searching. By default, all columns are selected:

- **Time**
- **Scanned folder**
- **Event**
- **User**

Record types: Choose one or more record log types from the drop-down menu:

- **Diagnostic** - Logs information needed to fine-tune the program and all records above.
- **Informative** - Records informative messages, including successful update messages, plus all records above.
- **Warnings** - Records critical errors and warning messages.
- **Errors** - Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** - Logs only critical errors (error starting antivirus protection).

Time period: Define the time period from which you want the results to be displayed.

- **Not specified** (default) - does not search within time period, searches the whole log.
- **Last day**
- **Last week**
- **Last month**
- **Time period** - you can specify the exact time period (date and time) to search only those records from a specified time period.

Match whole words only - Finds only records that match the string as a whole word in the **What** text box.

Match case sensitive - Finds only records that match the string with exact capitalization in the **What** text box.

Search upwards - Searches from the current position upwards.

Once you have configured your search options, click **Find** to start searching. The search stops when it finds the first corresponding record. Click **Find** again to see additional records. The Log files are searched from top to bottom, starting from your current position (the record that is highlighted).

5.6.7 Proxy server

In large LAN networks, the connection of your computer to the Internet can be mediated by a proxy server. If this is the case, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET Mail Security, proxy server setup is available in two different sections within the Advanced setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Mail Security. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, turn on the **Use proxy server** switch and then enter the address of the proxy server into the **Proxy server** field, along with the **Port** number of the proxy server.

If communication with the proxy server requires authentication, turn the **Proxy server requires authentication** switch on and enter a valid **Username** and **Password** into the respective fields. Click **Detect** to automatically detect and populate proxy server settings. The parameters specified in Internet Explorer will be copied.

NOTE: This feature does not retrieve authentication data (username and password); it must be supplied by you.

Proxy server settings can also be established within Advanced update setup (**Advanced setup** > **Update** > **HTTP Proxy** by selecting **Connection through a proxy server** from **Proxy mode** drop-down menu). This setting applies for the given update profile and is recommended for laptops that often receive virus signature updates from different locations. For more information about this setting, see the section Advanced update setup.

5.6.8 Email notifications

ESET Mail Security can automatically send notification emails if an event with the selected verbosity level occurs. Enable **Send event notifications by email** to activate email notifications.

NOTE: SMTP servers with TLS encryption are supported by ESET Mail Security.

- **SMTP server -** The SMTP server used for sending notifications.
- **Username and password -** If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.
- **Sender address** - Enter sender's address that will appear in the header of notification emails. This is what recipient will see as **From**.
- **Recipient address -** Specify recipient's email address **To** whom notifications will be delivered.
- **Minimum verbosity for notifications** - Specifies the minimum verbosity level of notifications to be sent.
- **Enable TLS** - Enable alert and notification messages supported by TLS encryption.
- **Interval after which new notification emails will be sent (min)** - Interval in minutes after which new notification will be sent via email. Set this value to 0 if you want to send those notifications immediately.
- **Send each notification in a separate email** - When enabled, the recipient will receive a new email for each individual notification. This may result in a large number of emails being received in a short period of time.

Message format

- **Format of event messages** - Format of event messages that are displayed on remote computers. Also see Edit format.
- **Format of threat warning messages** - Threat alert and notification messages have a predefined default format. We

advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format. Also see Edit format.

- **Use local alphabetic characters -** Converts an email message to the ANSI character encoding based on Windows Regional settings (for example, windows-1250). If you leave this deselected, a message will be converted and encoded in ACSII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?").
- **Use local character encoding -** The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

5.6.8.1 Message format

Communications between the program and a remote user or system administrator are done via emails or LAN messages (using the Windows® messaging service). The default format of the alert messages and notifications will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

Keywords (strings separated by % signs) are replaced in the message by the actual information as specified. The following keywords are available:

- **%TimeStamp%** - Date and time of the event
- **%Scanner%** - Module concerned
- **%ComputerName%** - Name of the computer where the alert occurred
- **%ProgramName%** - Program that generated the alert
- **%InfectedObject%** - Name of infected file, message, etc
- **%VirusName%** - Identification of the infection
- **%ErrorDescription%** - Description of a non-virus event

The keywords **%InfectedObject%** and **%VirusName%** are only used in threat warning messages, and **%ErrorDescription%** is only used in event messages.

5.6.9 Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by antivirus activity. When enabled, all pop-up windows are disabled and scheduled tasks are not run. System protection still runs in the background, but does not require any user interaction.

Click **Setup** > **Computer** and then click the switch next to **Presentation mode** to enable presentation mode manually. In **Advanced setup** (F5), click **Tools** > **Presentation mode**, and then click the switch next to **Enable Presentation mode when running applications in full-screen mode automatically** to have ESET Mail Security engage Presentation mode automatically when full-screen applications are run. Enabling Presentation mode is a potential security risk, so the protection status icon in the taskbar will turn orange and display a warning. You will also see this warning in the main program window where you will see **Presentation mode enabled** in orange.

When **Enable Presentation mode when running applications in full-screen mode automatically** is engaged, Presentation mode will start whenever you initiate a full-screen application and will automatically stop after you exit the application. This is especially useful for starting Presentation mode immediately after starting a game, opening a full screen application or starting a presentation.

You can also select **Disable Presentation mode automatically after** to define the amount of time in minutes after which Presentation mode will automatically be disabled.

5.6.10 Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, *ekrn*). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET Mail Security problems. Click the drop-down menu next to **Dump type** and select one of three available options:

- Select **Disable** (default) to disable this feature.
- **Mini** - Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited. However, because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- **Full** - Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

Target directory - Directory where the dump during the crash will be generated.

Open diagnostics folder - Click **Open** to open this directory within a new *Windows explorer* window.

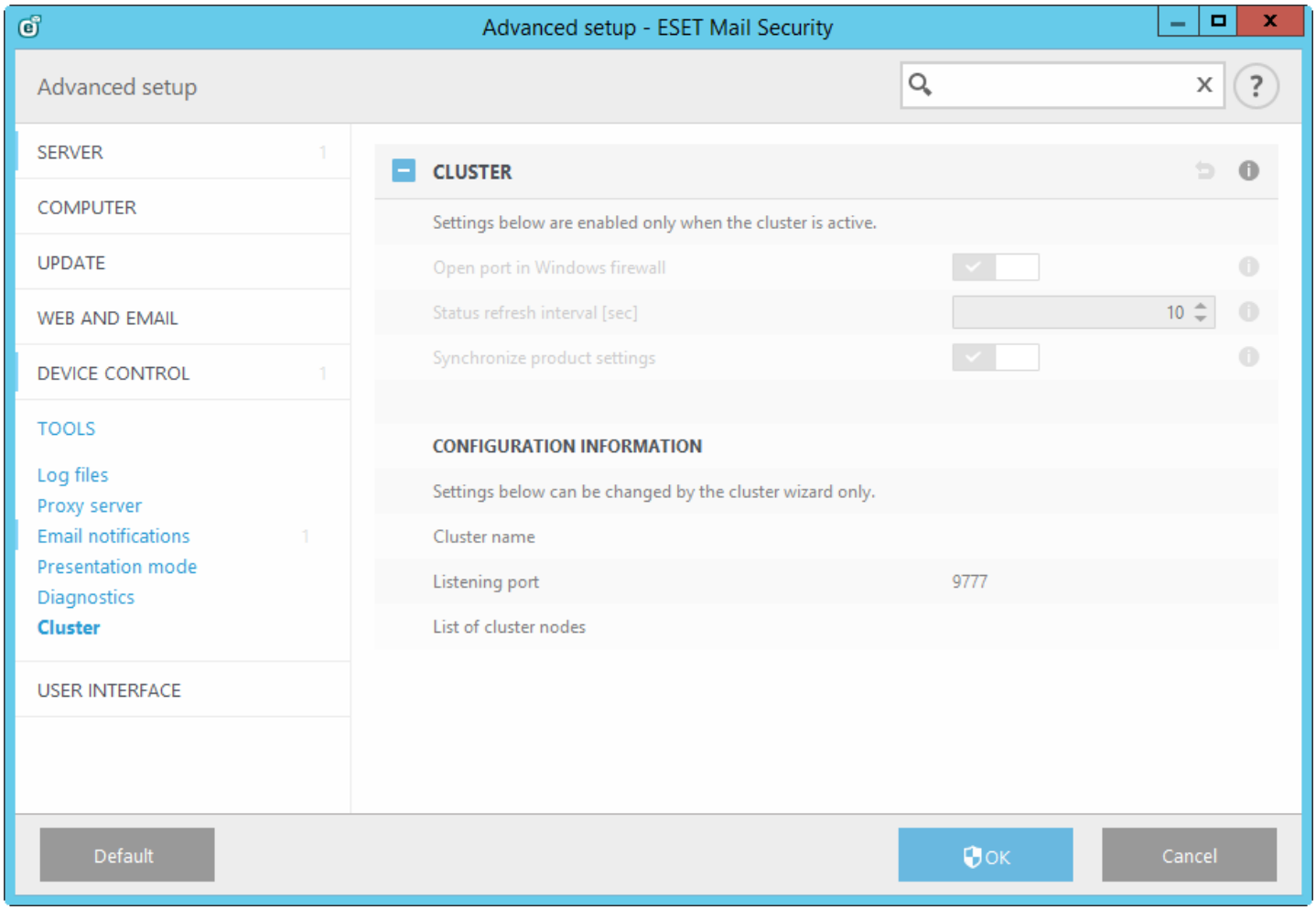
5.6.11 Customer Care

Submit system configuration data - Select **Always submit** from the drop-down menu, or select **Ask before submission** to be prompted before submitting data.

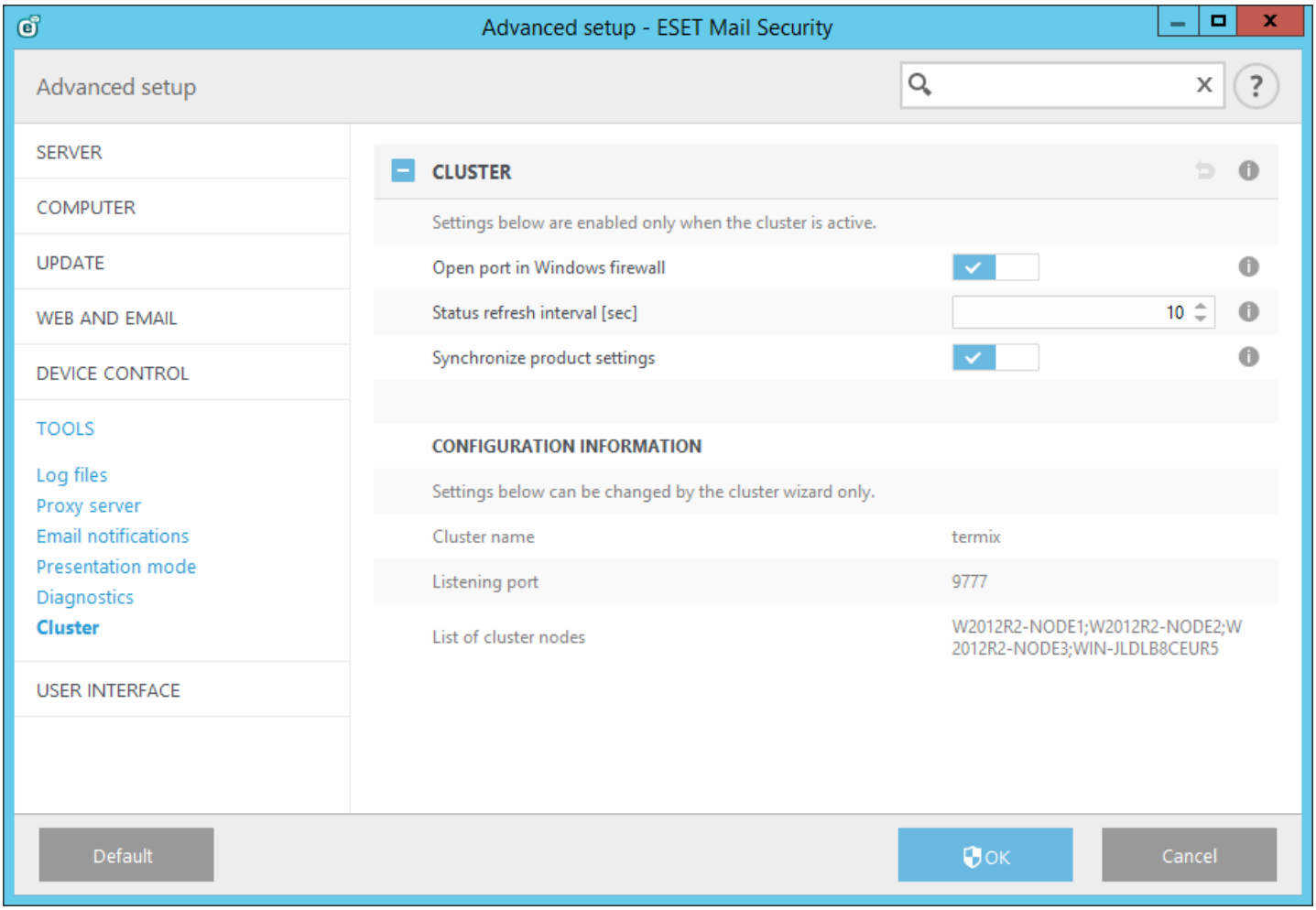
5.6.12 Cluster

Enable Cluster is automatically enabled when the ESET Cluster is configured. You can disable it manually in the Advanced setup window by clicking the switch icon (it is suitable when you need to change configuration without affecting other nodes in the ESET Cluster). This switch only enables or disables the ESET Cluster functionality. To properly set up or destroy the cluster, it is necessary to use the Cluster wizard or Destroy the cluster located in the **Tools** > **Cluster** section of the main program window.

ESET Cluster not configured and disabled:



ESET Cluster properly configured with its details and options:



For more information on the ESET Cluster click here.

5.7 User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI). You can adjust the program's visual appearance and effects.

To provide maximum security of your security software, you can prevent any unauthorized changes using the Access setup tool.

By configuring Alerts and notifications, you can change the behavior of detected threat alerts and system notifications. These can be customized to fit your needs.

If you choose not to display some notifications, they will be displayed in the Disabled messages and statuses area. Here you can check their status, show more details or remove them from this window.

Context menu integration is displayed after right-clicking selected object. Use this tool to integrate ESET Mail Security control elements into the context menu.

Presentation mode is useful for users who want to work with an application and not be interrupted by pop-up windows, scheduled tasks and any components that might stress system resources.

User interface elements

User interface configuration options in ESET Mail Security allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface** > **User interface elements** branch of the ESET Mail Security Advanced setup tree.

In the **User interface elements** section you can adjust the working environment. User interface should be set to **Terminal** if graphical elements slow the performance of your computer or cause other problems. You may also want

to turn off the GUI on a Terminal server. Fore more information about ESET Mail Security installed on Terminal server, see Disable GUI on Terminal Server topic.

Click the **Start mode** drop-down menu to select from the following Start modes:

- **Full** - The complete GUI will be displayed.
- **Terminal** - No notifications or alerts will be displayed. GUI can only be started by the Administrator.

If you want to deactivate the ESET Mail Security splash-screen, deselect **Show splash-screen at startup**.

To have ESET Mail Security play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select **Use sound signal**.

Integrate into the context menu - Integrate the ESET Mail Security control elements into the context menu.

Statuses - Click Edit to manage (enable or disable) statuses that are displayed in the Monitoring pane in main menu.
Application statuses - Allows you to enable or disable display status in the **Protection status** pane in main menu.

License Information - Enable this the license information, messages and notifications enable this option.

5.7.1 Alerts and notifications

The **Alerts and notifications** section under **User interface** allows you to configure how threat alerts and system notifications (e.g. successful update messages) are handled by ESET Mail Security. You can also set the display time and transparency of system tray notifications (this applies only on systems that support system tray notifications).

Alert windows

Disabling **Display alerts** will cancel all alert windows, and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left in its default setting (enabled).

Desktop notifications

Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select **Display notifications on desktop**. More detailed options, such as notification display time and window transparency can be modified below.

Turn the **Do not display notifications when running applications in full screen mode** switch on to suppress all non-interactive notifications.

The **Minimum verbosity of events to display** drop-down menu allows you to select the severity level of alerts and notification to be displayed. The following options are available:

- **Diagnostic** - Logs information needed to fine-tune the program and all records above.
- **Informative** - Records informative messages, including successful update messages, plus all records above.
- **Warnings** - Records critical errors and warning messages.
- **Errors** - Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** - Logs only critical errors (error starting antivirus protection, etc.).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies which user will receive system and other notifications on systems allowing multiple users to connect at the same time. Normally, this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

Message boxes

To close pop-up windows automatically after a certain period of time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time period elapses.

5.7.2 Access setup

In order to provide maximum security for your system, it is essential that ESET Mail Security is correctly configured. Any unqualified change may result in a loss of important data. To avoid unauthorized modifications, the setup parameters of ESET Mail Security can be password protected. Configuration settings for password protection are located in the **Access setup** submenu under **User interface** in the Advanced setup tree.

Password protect settings - Locks/unlocks the program's setup parameters. Click to open the Password setup window.

To set or change a password to protect setup parameters, click **Set password**.

Require full administrator rights for limited administrator accounts - Select this option to prompt the current user (if he or she does not have administrator rights) to enter administrator username and password when modifying certain system parameters (similar to the UAC in Windows Vista). The modifications include disabling protection modules.

5.7.2.1 Password

To avoid unauthorized modification, the setup parameters of ESET Mail Security can be password protected.

5.7.2.2 Password setup

To protect the setup paramaters of ESET Mail Security in order to avoid unauthorized modification, a new password must be set. When you want to change an existing password, type your old password in the **Old password** field, enter your new password in the **New password** and **Confirm password** fields and then click **OK**. This password will be required for any future modifications to ESET Mail Security.

5.7.3 Help

When you press the **F1** key or click the **?** button, an online help window will open. This is the primary source of help content. However, there is also an offline copy of help that comes installed with the program. Offline help opens in cases such as when there is no connection to the Internet.

The latest version of Online help will automatically be displayed when you have a working internet connection.

5.7.4 ESET Shell

You can configure access rights to product settings, features and data via eShell by changing the **ESET Shell execution policy**. The Default setting is **Limited scripting**, but you can change it to **Disabled**, **Read only** or **Full access** if needed.

- **Disabled** - eShell cannot be used at all. Only the configuration of eShell itself is allowed - in `ui eshell` context. You can customize the appearance of eShell, but cannot access product settings or data.
- **Read-only** - eShell can be used as a monitoring tool. You can view all settings in both Interactive and Batch mode, but you cannot modify any settings or features or modify any data.
- **Limited scripting** - in Interactive mode, you can view and modify all settings, features and data. In Batch mode eShell will function as if you were in Read-only mode, however if you use signed batch files, you will be able to edit settings and modify data.
- **Full access** - access to all settings is unlimited in both Interactive and Batch mode. You can view and modify any setting. You must use an administrator account to run eShell with full access. If UAC is enabled, elevation is also required.

5.7.5 Disable GUI on Terminal Server

This chapter describes how to disable GUI of ESET Mail Security running on Windows Terminal Server for user sessions.

Normally, ESET Mail Security GUI starts up every time a remote user logs onto the server and creates a terminal session. This is usually undesirable on Terminal Servers. If you want to turn off the GUI for terminal sessions, you can do so via eShell by running `set ui ui gui-start-mode terminal` command. This will put GUI into terminal mode. These are the two available modes for GUI startup:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

If you want to find out what mode is currently used, run `get ui ui gui-start-mode` command.

NOTE: In case you have installed ESET Mail Security on a Citrix server, we recommend you to use settings described in our KB article.

5.7.6 Disabled messages and statuses

Confirmation messages - Shows you a list of confirmation messages that you can select to display or not to display.

Disabled application statuses - Allows you to enable or disable display status in the **Protection status** pane in main menu.

5.7.6.1 Confirmation messages

This dialog window displays confirmation messages that ESET Mail Security will display before any action is performed. Select or deselect the check box next to each confirmation message to allow or disable it.

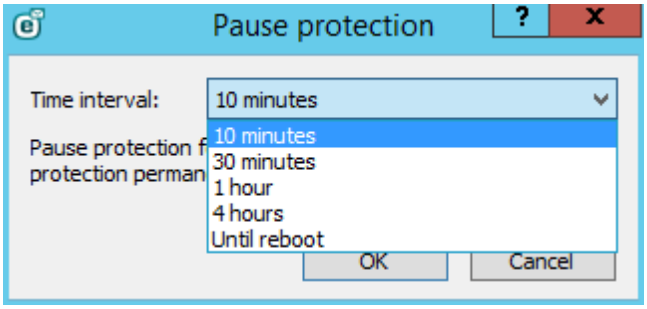
5.7.6.2 Disabled application statuses

In this dialog window you can select or deselect which application statuses will be or will not be displayed. For example, when you pause Antivirus and antispyware protection or when you enable Presentation mode. An application status will also be displayed if your product is not activated or if you license has expired.

5.7.7 System tray icon

Some of the most important setup options and features are available by right-clicking the system tray icon.

Pause protection - Displays the confirmation dialog box that disables Antivirus and antispyware protection, which guards against attacks by controlling file, web and email communication.



The **Time interval** drop-down menu represents the period of time that Antivirus and antispyware protection will be disabled for.

Advanced setup - Select this option to enter the **Advanced setup** tree. You can also access Advanced setup by pressing the F5 key or navigating to **Setup** > **Advanced setup**.

Log files - Log files contain information about all important program events that have occurred and provide an overview of detected threats.

Hide ESET Mail Security - Hide the ESET Mail Security window from the screen.

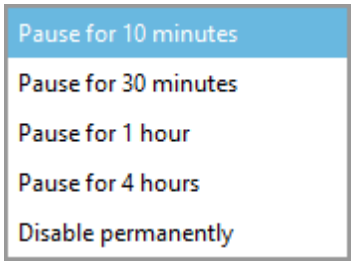
Reset window layout - Resets the ESET Mail Security window to its default size and position on the screen.

Virus signature database update - Starts updating the virus signature database to ensure your level of protection against malicious code.

About - Provides system information, details about the installed version of ESET Mail Security and the installed program modules as well as your license expiration date. Information about your operating system and system resources can be found at the bottom of the page.

5.7.7.1 Pause protection

Any time that you temporarily pause the Antivirus and antispyware protection sing the system tray icon, the **Temporarily pause protection** dialog box will appear. This will disable malware-related protection for the selected time period (to disable protection permanently, you must use Advanced setup). Use caution, disabling protection can expose your system to threats.

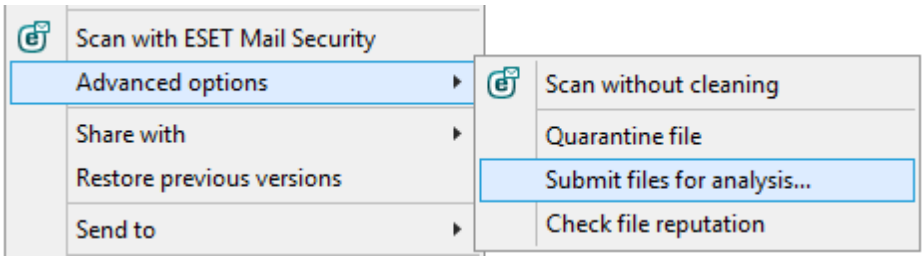


5.7.8 Context menu

The context menu is displayed after right-clicking an object (file). The menu lists all of the actions that you can perform on an object.

It is possible to integrate ESET Mail Security control elements into the context menu. Setup option for this functionality are available in the Advanced setup tree under **User Interface** > **User interface elements**.

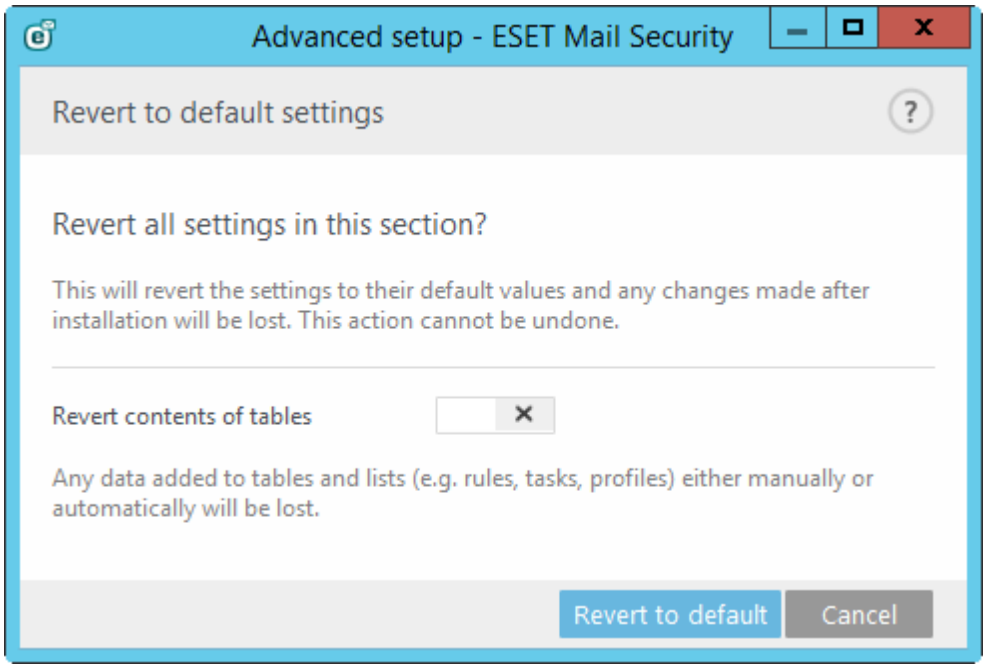
Integrate into the context menu - Integrate the ESET Mail Security control elements into the context menu.



5.8 Revert all settings in this section

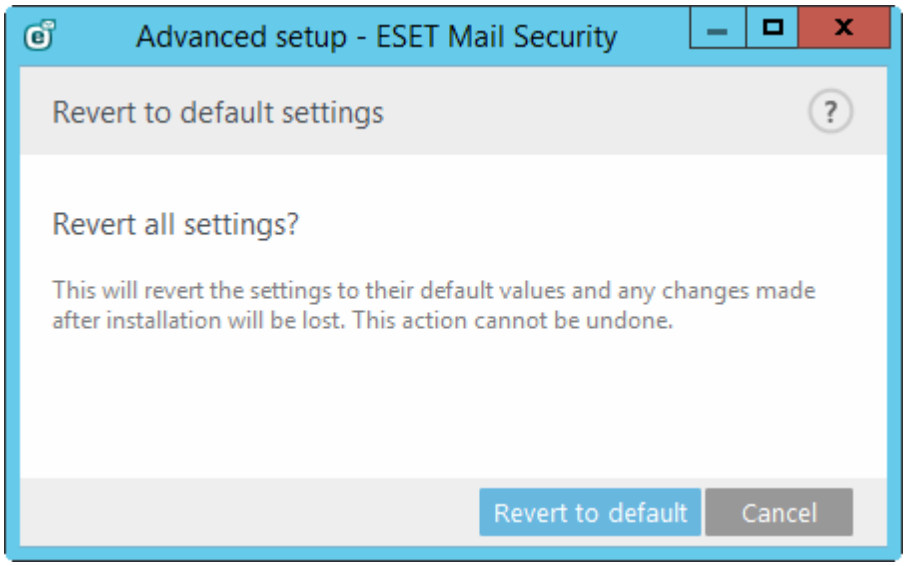
Reverts module settings to the default settings defined by ESET. Please note, any changes that have been made will be lost after you click **Revert to default**.

Revert contents of tables - When enabled, the rules, tasks or profiles that have been added manually or automatically will be lost.


Advanced setup - ESET Mail Security
Revert to default settings
Revert all settings in this section?
This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.
Revert contents of tables
Any data added to tables and lists (e.g. rules, tasks, profiles) either manually or automatically will be lost.
Revert to default
Cancel

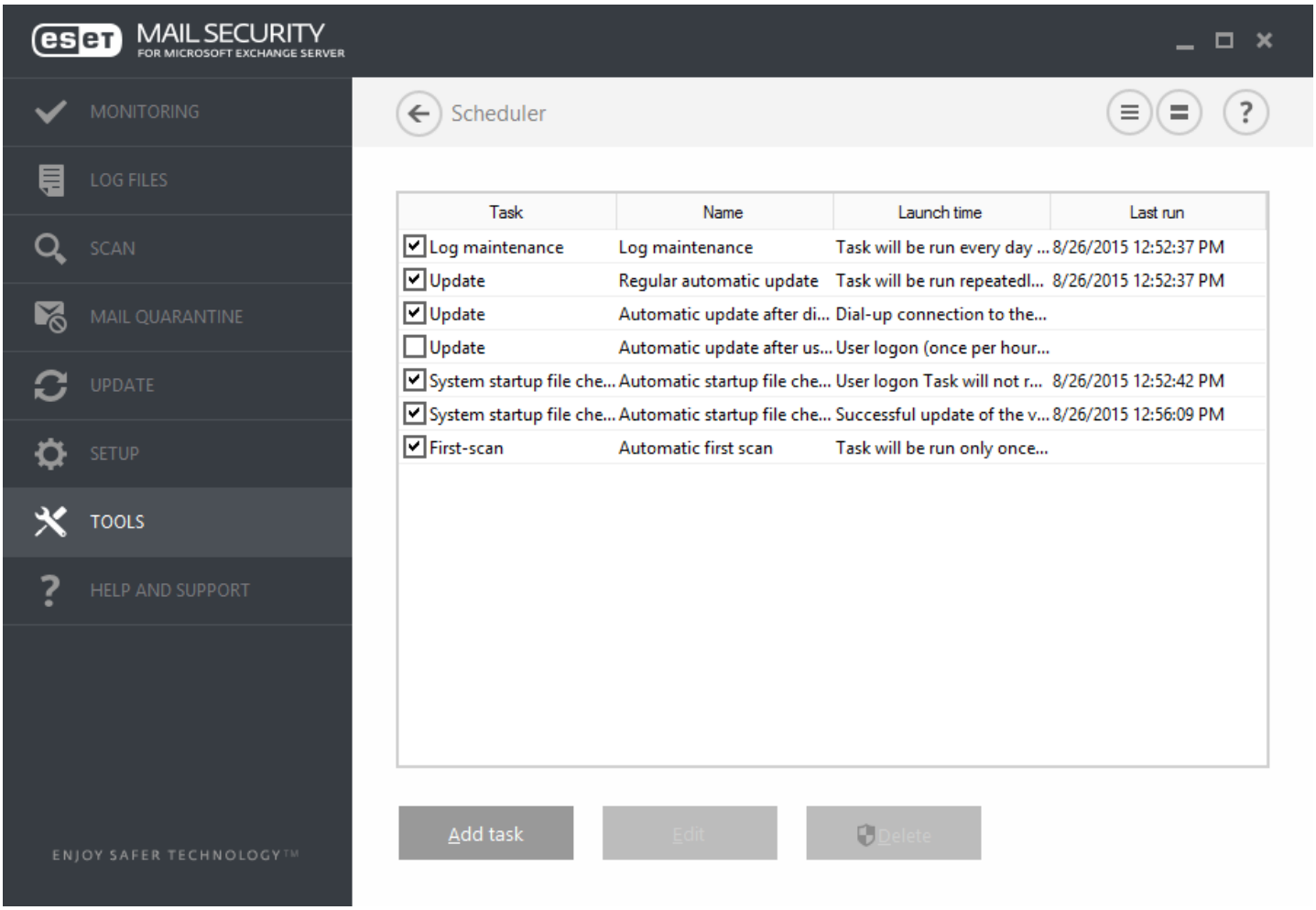
5.9 Revert to default settings

All program settings, for all modules, will be reset to the status they would have had after a new installation.


Advanced setup - ESET Mail Security
Revert to default settings
Revert all settings?
This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.
Revert to default
Cancel

5.10 Scheduler

Scheduler can be found in the ESET Mail Security main menu under **Tools**. Scheduler contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.



By default, the following scheduled tasks are displayed in **Scheduler**:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check (after user logon)**
- **Automatic startup file check (after successful update of the virus signature database)**
- **Automatic first scan**

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit...** or select the desired task you wish to modify and click the **Edit...** button.

5.10.1 Task details

Enter the name of the task and select one of the **Task type** option and then click **Next**:

- **Run external application** - Schedules the execution of an external application.
- **Log maintenance** - Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** - Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** - Creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** - Performs a computer scan of files and folders on your computer.
- **First scan** - By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** - Schedules an Update task by updating the virus signature database and program modules.
- **Database scan** - Lets you schedule a Database scan and choose items that will be scanned. It is basically an On-demand database scan.

NOTE: If you have Mailbox database protection enabled, you can still schedule this task, but it will end up with an error message displayed in Scan section of the main GUI saying Database scan - Scan interrupted because of an error. To prevent this, you need to ensure that Mailbox database protection is disabled during the time **Database scan** is scheduled to run.

- **Send mail quarantine reports** - Schedules a Mail Quarantine report to be sent via email.
- **Background scan** - Gives Exchange Server an opportunity to run database background scan if needed.

- Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting check box in the list of scheduled tasks).
- Click **Next** and select one of the timing options: Once, Repeatedly, Daily, Weekly and Event triggered. Based on the frequency selected, you will be prompted with different update parameters.
- A task can be **skipped when computer is running on battery power** or is powered off.
- **Next**, define what action to take if the task cannot be performed or completed at the scheduled time.

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

5.10.2 Task timing - Once

Task execution - The specified task will be run only once at the specified date and time.

5.10.3 Task timing

The task will be performed repeatedly at the specified time interval. Select one of the timing options:

- **Once** - The task will be performed only once at the predefined date and time.
- **Repeatedly** - The task will be performed at the specified interval (in hours).
- **Daily** - The task will run each day at the specified time.
- **Weekly** - The task will run one or more times a week, on the selected day(s) and time.
- **Event triggered** - The task will be performed after a specified event.

Skip task when running on battery power - A task will not start if your computer is running on battery at the moment the task should launch. This also applies to computers running on UPS.

5.10.4 Task timing - Daily

The task will run repeatedly each day at the specified time.

5.10.5 Task timing - Weekly

The task will run on the selected day and time.

5.10.6 Task timing - Event triggered

The task can be triggered by any of the following events:

- **Every time the computer starts**
- **The first time the computer starts each day**
- **Dial-up connection to the Internet/VPN**
- **Successful update of the virus signature database**
- **Successful update of the program components**
- **User logon**
- **Threat detection**

When scheduling a task triggered by an event, you can specify the minimum interval between two completions of the task. For example, if you log on to your computer several times a day, choose 24 hours to perform the task only on the first logon of the day and then the next day.

5.10.7 Task details - Run application

This task schedules the execution of an external application.

- **Executable file** - Choose an executable file from the directory tree, click the **...** option or enter the path manually.
- **Work folder** - Define the external application's working directory. All temporary files of the selected **Executable file** will be created within this directory.
- **Parameters** - Command line parameters for the application (optional).

Click **Finish** to apply the task.

5.10.8 Task details - Send mail quratine reports

This task schedules a Mail Quarantine report to be sent via email.

- **Sender address** - Specify an email address which will displayed as a sender of the Mail Quarantine report.
- **Max count of records in report** - You can limit the number of entries per report. Default count is set to 50.
- **Web URL** - This URL will be included in the Mail Quarantine report so that the recipient can simply click it to access the Web interface of Mail Quarantine.
- **Recipients** - Choose users who will be receiving Mail Quarantine reports. Click **Edit** to select the mailboxes for specific recipients. You can select multiple recipients.

Click **Finish** to create the scheduled task.

5.10.9 Skipped task

If the task could not be run at the predefined time, you can specify when it will be performed:

- **At the next scheduled time** - The task will be executed at the specified time (for example after 24 hours).
- **As soon as possible** - The task will run as soon as possible - when the actions that prevent the task from executing are no longer valid.
- **Immediately, if time since last run exceeds a specified value** - **Time since last run (hours)** - After you select this option, your task will be always repeated after the specified amount of time (in hours).

5.10.10 Scheduler task details

This dialog window displays detailed information about the selected scheduled task when you double-click on a custom task or right-click on a custom scheduler task and click **Show task details**.

5.10.11 Scheduler task - Background scan

Background scan - This task type allows for database scan via VSAPI in the background. It basically lets your Exchange Server to run background scan if needed. The scan is triggered by the Exchange Server itself, this means that it is up to the Exchange Server whether the scan will be executed within allowed time.

We recommend you to allow this task to run outside of peak hours when your Exchange Server is not busy, for example during night-time. This is because the database background scan might puts certain amount of load on your system. Also, the time frame should not collide with any backups that might be running on your Exchange Server in order to prevent performance or availability issues.

NOTE: Mailbox database protection must be enabled in order for the scheduled task to run. This type of protection is only available for Microsoft Exchange Server 2010, 2007 and 2003 operating in the Mailbox Server (Microsoft Exchange 2010 and 2007) or Back-End server (Microsoft Exchange 2003) role.

Timeout (hours) - Specify how many hours is your Exchange Server allowed to run the database background scan from the time this scheduled task is executed. Once it reaches the timeout, Exchange will be instructed to stop its background scan.

5.10.12 Update profiles

If you wish to update the program from two update servers, then it is necessary to create two different update profiles. If the first one fails to download update files, then the program automatically switches to the alternative one. This is suitable, for example, for notebooks which normally update from a local LAN update server, but their owners often connect to the Internet using other networks. So, if the first profile fails, the second one will automatically download update files from ESET's update servers.

You will find more information on update profiles in chapter Update.

5.10.13 Creating new tasks

To create a new task in Scheduler, click the **Add task** button or right-click and select **Add** from the context menu. Five types of scheduled tasks are available:

- **Run external application** - Schedules the execution of an external application.
- **Log maintenance** - Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** - Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** - Creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** - Performs a computer scan of files and folders on your computer.
- **First scan** - By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** - Schedules an Update task by updating the virus signature database and program modules.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task.

Enter a name of the task into the **Task name** field. From the **Task type** drop-down menu select **Update** and click **Next**.
Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting check box in the list of scheduled tasks), click **Next** and select one of the timing options:
Once, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if time since last exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

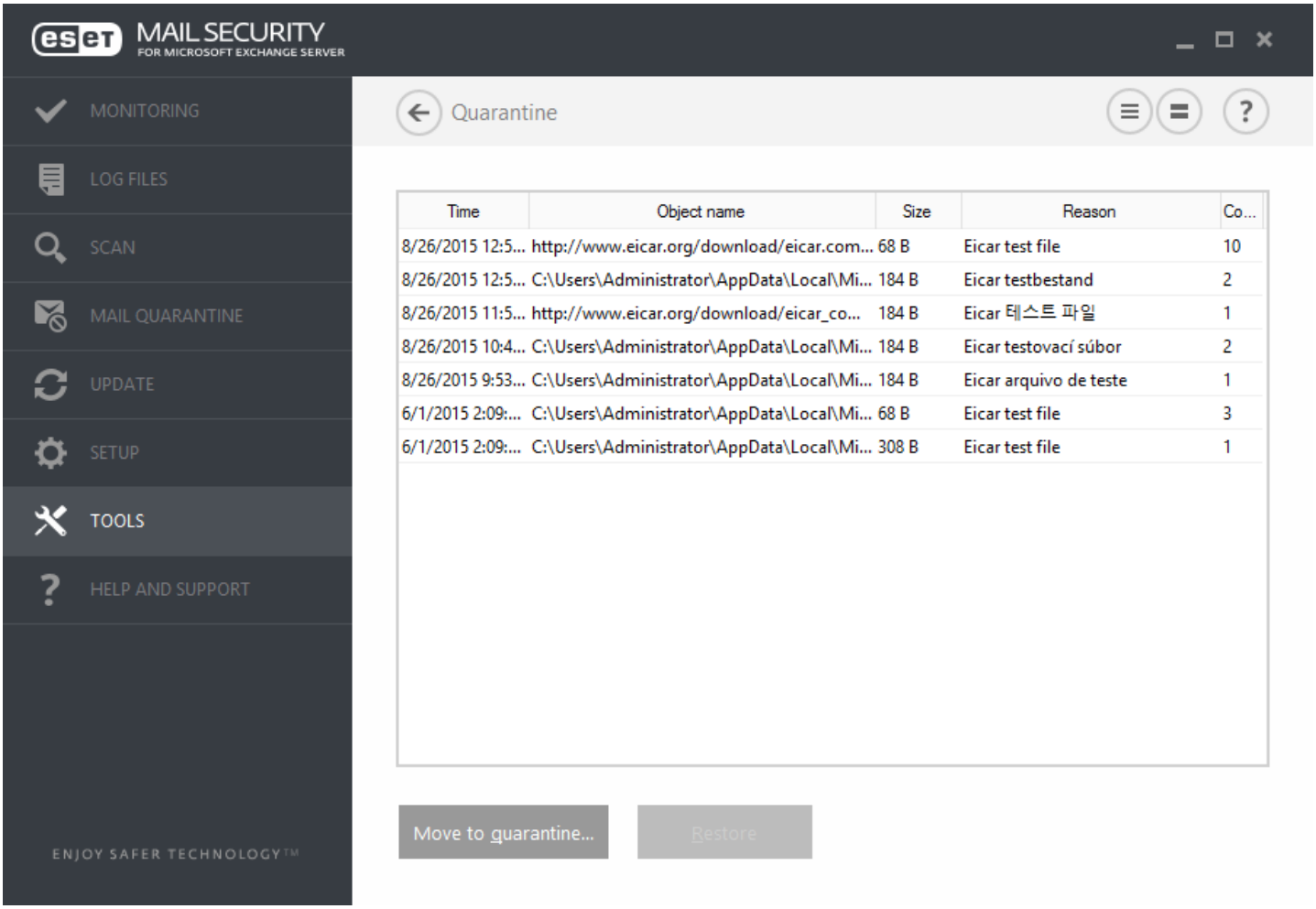
In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of scheduled tasks.

5.11 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET Mail Security.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.



Files stored in the quarantine folder can be viewed in a table that displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (for example, object added by user), and number of threats (for example, if it is an archive containing multiple infiltrations).

In case email message objects are quarantined in the file quarantine, information in a form of path to the mailbox/folder/filename is displayed.

Quarantining files

ESET Mail Security automatically quarantines deleted files (if you have not disabled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Quarantine.** Quarantined files will be removed from their original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine**.

Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature, available from the context menu by right-clicking a given file in the Quarantine window, to do so. If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option will be available. Read more about this type of application in the glossary. The context menu also offers the **Restore to...** option which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantines a harmless file by mistake, please exclude the file from scanning after restoring it and send the file to ESET Customer Care.

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

5.11.1 Quarantining files

ESET Mail Security automatically quarantines deleted files (if you have not disabled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Quarantine**. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose right-click in the **Quarantine** window and select **Quarantine**.

5.11.2 Restoring from Quarantine

Quarantined files can also be restored to their original location. To restore a quarantined file, right-click it in the Quarantine window and select **Restore** from the context menu. If a file is marked as a potentially unwanted application, **Restore and exclude from scanning** will also be available. The context menu also contains the **Restore to...** option, which allows you to restore a file to a location other than the one from which it was deleted.

Deleting from Quarantine - Right-click on a given item and select **Delete from Quarantine**, or select the item you want to delete and press **Delete** on your keyboard. You can also select multiple items and delete them together.

NOTE: If the program has quarantined a harmless file by mistake, exclude the file from scanning after restoring it and send the file to ESET Customer Care.

5.11.3 Submitting file from Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Threat Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

5.12 Operating system updates

The System updates window shows the list of available updates ready to be downloaded and installed. The update priority level is shown next to the name of the update.

Click **Run system update** to start downloading and installing operating system updates.

Right-click any update row and click **Show information** to display a pop-up window with additional info.

6. Glossary

6.1 Types of infiltration

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

6.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses mainly attack executable files and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program by him/herself.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage - they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state - i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

6.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves - they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes of their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

6.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past- oday, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. “Trojan horse” has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- **Downloader** - A malicious program with the ability to download other infiltrations from the Internet
- **Dropper** - A type of trojan horse designed to drop other types of malware onto compromised computers
- **Backdoor** - An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it
- **Keylogger** - (keystroke logger) - A program which records each keystroke that a user types and sends the information to remote attackers
- **Dialer** - Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader. Small.ZL, Slapper.

6.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data, etc. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2) When they are hidden from the usual testing. ESET Mail Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

6.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser’s home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous - users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a “legal” way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory - they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.7 Packers

A packer is a runtime self-extracting executable that combines several kinds of malware into a single package.

The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

6.1.8 Exploit Blocker

Exploit Blocker is designed to fortify commonly exploited applications such as web browsers, PDF readers, email clients or MS Office components. It monitors behavior of processes for suspicious activity that might indicate an exploit. It adds another layer of protection, one step closer to attackers, by using a completely different technology compared to techniques focusing on detection of malicious files themselves.

When Exploit Blocker identifies a suspicious process, it can stop the process immediately and record data about the threat, which is then sent to the ESET LiveGrid cloud system. This data is processed by the ESET Threat Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware for which there is no pre-configured remedy).

6.1.9 Advanced Memory Scanner

Advanced Memory Scanner works in combination with Exploit Blocker to provide better protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation and/or encryption. In cases where ordinary emulation or heuristics might not detect a threat, the Advanced Memory Scanner is able to identify suspicious behavior and scan threats when they reveal themselves in system memory. This solution is effective against even heavily obfuscated malware. Unlike Exploit Blocker, this is a post-execution method, which means that there is a risk that some malicious activity could have been performed prior to its detecting a threat. However in the case that other detection techniques have failed, it offers an additional layer of security.

6.1.10 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET Mail Security provides the option to detect such threats.

Potentially unsafe applications is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

6.1.11 Potentially unwanted applications

Potentially unwanted applications (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent before installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously (pop-ups, ads)
- Activating and running of hidden processes
- Increased usage of system resources
- Changes in search results
- Application communicates with remote servers

6.2 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software - malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases - with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms - be especially cautious of options such as "Yes, I want to receive information".
- Use "specialized" email addresses - e.g., one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

6.2.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

6.2.2 Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

6.2.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data - bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

6.2.4 Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message:

- Sender address does not belong to someone on your contact list
- You are offered a large sum of money, but you have to provide a small sum first
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data - bank account numbers, usernames and passwords, etc.
- It is written in a foreign language
- You are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable id (consult the original product manufacturer)
- Some of the words are misspelled in an attempt to trick your spam filter. For example "vaigra" instead of "viagra",

etc

6.2.4.1 Rules

In the context of Antispam solutions and email clients, rules are tools for manipulating email functions. They consist of two logical parts:

1) Condition (e.g., an incoming message from a certain address)

2) Action (e.g., deletion of the message, moving it to a specified folder)

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

- Condition: An incoming email message contains some of the words typically seen in spam messages 2. Action: Delete the message
- Condition: An incoming email message contains an attachment with an .exe extension 2. Action: Delete the attachment and deliver the message to the mailbox
- Condition: An incoming email message arrives from your employer 2. Action: Move the message to the “Work” folder

We recommend that you use a combination of rules in Antispam programs in order to facilitate administration and to more effectively filter spam.

6.2.4.2 Bayesian filter

Bayesian spam filtering is an effective form of email filtering used by almost all Antispam products. It is able to identify unsolicited email with high accuracy and can work on a per-user basis.

The functionality is based on the following principle: The learning process takes place in the first phase. The user manually marks a sufficient number of messages as legitimate messages or as spam (normally 200/200). The filter analyzes both categories and learns, for example, that spam usually contains the words “rolex” or “viagra”, and legitimate messages are sent by family members or from addresses in the user’s contact list. Provided that a sufficient number of messages are processed, the Bayesian filter is able to assign a specific “spam index” to each message in order to determine whether it is spam or not.

The main advantage of a Baysesian filter is its flexibility. For example, if a user is a biologist, all incoming emails concerning biology or relative fields of study will generally receive a lower probability index. If a message includes words that would normally qualify it as unsolicited, but it is sent by someone from the user’s contact list, it will be marked as legitimate, because senders from a contact list decrease overall spam probability.

6.2.4.3 Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted permission. The term “email whitelist“ defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in “exclusivity mode“, then messages from any other address, domain, or IP address will not be received. If a whitelist is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a blacklist. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

6.2.4.4 Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist. Those created by users within their Antispam application, and a professional, regularly updated blacklists which are created by specialized institutions and can be found on the Internet.

It is essential to use blacklists to successfully block spam, but they are difficult to maintain, since new items to be blocked appear every day. We recommended you use both a whitelist and a blacklist to most effectively filter spam.

6.2.4.5 Server-side control

Server-side control is a technique for identifying mass spam based on the number of received messages and the reactions of users. Each message leaves a unique digital “footprint” based on the content of the message. The unique ID number tells nothing about the content of the email. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored in the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.